

Industrial Automation and Control System Security Principles

Ronald L. Krutz, Ph.D., P.E.



Setting the Standard for Automation™

Industrial Automation and Control System Security Principles

Ronald L. Krutz, Ph.D., P.E.



Notice

The information presented in this publication is for the general education of the reader. Because neither the author(s) nor the publisher has any control over the use of the information by the reader, both the author(s) and the publisher disclaim any and all liability of any kind arising out of such use. The reader is expected to exercise sound professional judgment in using any of the information presented in a particular application.

Additionally, neither the author(s) nor the publisher has investigated or considered the effect of any patents on the ability of the reader to use any of the information in a particular application. The reader is responsible for reviewing any possible patents that may affect any particular use of the information presented.

Any references to commercial products in the work are cited as examples only. Neither the author(s) nor the publisher endorses any referenced commercial product. Any trademarks or tradenames referenced belong to the respective owner of the mark or name. Neither the author(s) nor the publisher makes any representation regarding the availability of any referenced commercial product at any time. The manufacturer's instructions on use of any commercial product must be followed at all times, even if in conflict with the information in this publication.

Copyright © 2013 International Society of Automation (ISA)

All rights reserved.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2

ISBN: 978-1-937560-63-8

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

ISA

67 Alexander Drive

P.O. Box 12277

Research Triangle Park, NC 27709

Library of Congress Cataloging-in-Publication Data in process

Dedication

*To the Pirate Munchkins who have captured my heart:
Patrick, Ryan, Aaron, and Emma*

Acknowledgment

I want to thank my wife, Hilda, for her encouragement and support during the writing of this book.

RLK

Contents

About the Author

Foreword

Preface – Industrial Automation and Control System Security: A Component of a Nation's Critical Infrastructure

Chapter 1 – Industrial Automation and Control System Fundamental Concepts

- Industrial Automation and Control Systems
- Industrial Automation and Control System Protocol Summary
- Issues in Industrial Automation and Control Systems Security
- Summary
- Review Questions for Chapter 1
- References

Chapter 2 – Information System Security Technology

- Information System Security Fundamentals
- Types and Classes of Attack
- Additional System Security Concepts
- Policies, Standards, Guidelines, and Procedures
- Malicious Code and Attacks
- Firewalls
- Cryptography
- Attacks Against Cryptosystems
- Virtual Private Network
- Summary
- Review Questions for Chapter 2
- References

Chapter 3 – Industrial Automation and Control System Culture versus IT Paradigms

- Differences in Culture, Philosophy, and Requirements
- Considerations in Adapting IT Security Methods to Industrial Automation and Control Systems
- IT and Industrial Automation and Control Systems Comparisons from a Standards Perspective
- Summary
- Review Questions for Chapter 3
- References

Chapter 4 – The Continuing Technological Evolution Affecting the Industrial Automation and Control Systems

Important Technological Trends

The Smart Grid and Technological Trends

Mapping of Emerging Technology Issues onto an Example Automation System – The Smart Grid

Summary

Review Questions for Chapter 4

References

Chapter 5 – Risk Management for Industrial Automation and Control Systems

Risk Management

The Insider Threat

Threat Examples Worthy of Note

Summary

Review Questions for Chapter 5

References

Chapter 6 – Industrial Automation and Control Systems Security Methodologies and Approaches

Automation and Control System Security Standards and Guidelines

NIST Special Publication 800-82, Guide to Industrial Control Systems Security

ANSI/ISA-TR99.00.01-2007, Security Technologies for Industrial Automation and Control Systems

North American Electric Reliability Corporation, Critical Infrastructure Protection Cybersecurity Standards

NIST Special Publication 800-53, Revision 3, Recommended Security Controls for Federal Information Systems

Department of Homeland Security, Catalog of Control Systems Security: Recommendations for Standards Developers

AMI System Security Requirements

Department of Defense Instruction Number 8500.2, Information Assurance (IA) Implementation

Consolidation of Best Practices Controls for Industrial Automation and Control Systems

Summary

Review Questions for Chapter 6

References

Chapter 7 – Industrial Automation and Control System Security Training

Background

Training Sources and Approaches

Training Support Guidelines

Common Training Subjects

Summary

Review Questions for Chapter 7

References

Chapter 8 – Future Industrial Automation and Control System Approaches and Issues

Automation and Control System Trends

Formal Methods Used to Quantify and Standardize Important Concepts and Applications

Future Smart Grid Issues and Automation Security Issues

Summary

Review Questions for Chapter 8

References

Appendix A – Review Questions and Answers

Glossary and Acronyms

Bibliography

About the Author

RONALD L. KRUTZ, Ph.D., P.E., CISSP, ISSEP

Dr. Krutz is Chief Scientist for Security Risk Solutions, Inc. He has more than thirty years of experience in industrial automation and control systems, distributed computing systems, computer architectures, information assurance methodologies, and information security training. He has been a Senior Information Security Consultant at Lockheed Martin, BAE Systems, and REALTECH Systems Corporation, an Associate Director of the Carnegie Mellon Research Institute (CMRI), and a professor in the Carnegie Mellon University Department of Electrical and Computer Engineering. He was also a lead instructor for (ISC)² Inc. in its Certified Information Systems Security Professionals (CISSP) training seminars. Dr. Krutz founded the CMRI Cybersecurity Center and was founder and Director of the CMRI Computer, Automation and Robotics Group.

He coauthored the CISSP Prep Guide for John Wiley and Sons and is coauthor of the *Wiley Advanced CISSP Prep Guide*; the *CISSP Prep Guide, Gold Edition*; the *Security + Certification Guide*; the *CISM Prep Guide*; the *CISSP Prep Guide, 2nd Edition: Mastering CISSP and ISSEP (Information Systems Security Engineering Professional)*; the *Network Security Bible*; the *CISSP and CAP (Certification and Accreditation Professional) Prep Guide, Platinum Edition: Mastering CISSP and CAP*; the *Certified Ethical Hacker (CEH) Prep Guide*; *Cloud Computing Security*; and *Web Commerce Security*. He is also the author of *Securing SCADA Systems* and of three textbooks in the areas of microcomputer system design, computer interfacing and computer architecture. Dr. Krutz has seven patents in the area of digital systems and has published more than 30 technical papers.

Dr. Krutz also serves as consulting editor for the John Wiley and Sons Information Security Certification Series and is a Senior Fellow of the International Cyber Center of George Mason University.

Dr. Krutz holds B.S., M.S., and Ph.D. degrees in Electrical and Computer Engineering and is a Registered Professional Engineer in Pennsylvania.

Foreword

Why should we care about the security of industrial automation and control systems? Surely these systems are isolated, segmented, and already well protected. After all, they control manufacturing plants, oil refineries, power plants, and other elements of our critical infrastructure. We know that we can't just casually saunter through the main entrance of a pipeline control center or power plant without the proper credentials ... but without adequate automation system security controls, the virtual back door may be wide open to uninvited visitors.

It's easy to recognize the potential for harm if industrial automation and control systems were to be manipulated by adversaries, and there are real-world scenarios that both demonstrate such capability and make it clear that there are individuals or organizations with the motive. An obvious example is the Stuxnet family of worms, which have targeted control systems including those purportedly used by Iranian organizations for uranium enrichment.

Industrial automation and control systems are a hidden but integral part of our daily lives. Their components include programmable logic controllers (PLCs), programmable automation controllers (PACs), intelligent electronic devices (IEDs), SCADA servers, and remote terminal units (RTUs), which respond with specific output signals based on the commands they receive. A simple example is a PLC that receives an input signal or command from a sensor, such as a temperature sensor on a machine in an industrial production line. When an alarm condition is detected, the output signal might shut down the machine to avoid overheating and potential damage or fire. With the widespread proliferation of computing and network technologies (e.g., high bandwidth wireless technology and broad availability of the public Internet), a natural evolution has been the development of software systems to monitor, control, and manage critical infrastructure and manufacturing systems.

So how do we figure out what the next Stuxnet, Duqu, Flame or other malicious code that targets industrial control systems might be capable of? What other threats to industrial automation and control systems exist (or may exist in the future) that our critical infrastructure might be vulnerable to, and what can we do about them?

To help answer these questions, Dr. Krutz describes the conditions that expose our critical infrastructure to network-based threats, and presents a method for identifying, prioritizing and mitigating the associated risk. Dr. Krutz seamlessly fuses his deep knowledge of information security risk management

techniques with his impressive engineering experience to articulate a readily actionable approach to improving the confidentiality, integrity and availability of industrial automation and control systems through effective risk management.

This book is a compelling eye-opener for organizational leaders and a “must read” for anyone involved in the management, engineering, or operation of any aspect of our critical infrastructure.

Johnathan Coleman
Principal, Security Risk Solutions Inc.

Preface

Industrial Automation and Control System Security: A Component of a Nation's Critical Infrastructure

As defined by ANSI/ISA-99.00.01, industrial automation and control systems (IACS) include (but are not limited to) distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA) systems, networked electronic sensing and control, and monitoring and diagnostic systems.

A SCADA system provides the ability to obtain information from remote installations and to send limited control commands to those installations. Industrial control systems (including DCSs, PLCs, and intelligent electronic devices) comprise real-time elements that control critical industrial processes in a wide variety of applications.

Before the advent of local area networking, computer-based industrial automation and control systems were generally isolated from the outside world and used their own proprietary communication protocols. Eventually, as networking technology improved, interconnectivity among plants and other corporate units emerged as a way of obtaining increased knowledge of plant operations and more efficient management of resources.

With the maturation of the Internet and browsers, the TCP/IP protocol and Ethernet LANs found their way into supervisory control and data acquisition systems as well as process and manufacturing plant control systems.

In addition, computing platforms such as PCs running Windows were adopted for reasons of lower cost and standardization. However, with these advantages came the disadvantages of vulnerabilities and exposure to threats that plague these platforms.

There is also an emerging trend in many organizations toward consolidating some overlapping activities in IACS and corporate IT systems. This trend is

motivated by the cost savings achievable by avoiding the use of disparate platforms, networks, software, and maintenance tools and by an increased capability to run the total organization more efficiently and effectively.

An important issue associated with the merging of these two systems is that, in many cases, both IACS and corporate IT environments use the same security model. This overlap introduces the possibility of the corporate Internet connection exposing critical operations to additional threats and compromising the real-time, deterministic requirements of plant control systems. The emergence of the Stuxnet worm, aimed specifically at PLCs that transmit and receive real-time control bits, highlights the sophisticated threats that exist today and the critical need for IACS-optimized system security methods. Follow-up malware such as the Flame or Flamer virus that have appeared portend a trend of future attacks on these critical systems.

This book develops a novel approach to securing industrial automation and control systems by generating applicable, useful, protection principles through the merging and adaptation of the best industrial and governmental standards and practices.

Chapter 1

Industrial Automation and Control System Fundamental Concepts

The material in this chapter provides basic coverage of industrial automation and control system components and terminology, including supervisory control and data acquisition (SCADA) systems and distributed control systems (DCSs). However, because the focus of this book is the security of these systems, this chapter is not designed to be a comprehensive tutorial on industrial automation and control systems. The material assumes that the reader is familiar with these systems and communications terminology.

Note that the term DCS is also used to refer to digital control systems, but, unless otherwise stated, in this book DCS will denote a distributed control system.

Industrial Automation and Control Systems

Over the years, as industrial automation and control systems have evolved into distributed control systems and SCADA systems, the associated terminology has meant different things to different people. Control engineers, software engineers, plant personnel, and management have attached different meanings to commonly used terms such as distributed control systems, industrial control systems (ICSs), supervisory control systems, and SCADA systems.

This situation has been further complicated by the migration from relay logic, to programmable logic controllers (PLCs), to microcomputers, to the use of local area networks, Windows platforms, standard buses, and so on.

To establish a solid foundation for the material in this book, the definitions from ANSI/ISA-99.00.01-2007¹ and NIST Special Publication 800-82² will be used.

ANSI/ISA-99.00.01 defines industrial control systems, distributed control systems, PLCs, and SCADA systems as belonging to the class of industrial automation and control systems (IACSs). Specifically, ANSI/ISA-99.00.01

states that an industrial automation and control system is:

A collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process. These systems include, but are not limited to:

a. industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety instrumented system [SIS] functions, whether they are physically separate or integrated.)

b. associated information systems, such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems.

c. associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

NIST SP 800-82 defines an industrial automation and control system as “a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and other control system configurations, such as skid-mounted programmable logic controllers (PLCs) often found in the industrial sectors and critical infrastructures.”

In this text, the ANSI/ISA-99.00.01 terminology and definitions will take precedence over others where there are differences.

SCADA Systems

ANSI/ISA-99.00.01 defines a SCADA system as “a type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems.” NIST SP 800-82 describes SCADA systems as:

Highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems, such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data.

ANSI C37.13 defines SCADA as a system operating with coded signals over communication channels to control remote terminal unit (RTU) equipment. The supervisory system may be combined with a data acquisition system by using coded signals over communication channels to acquire information about the status of RTU equipment for display or for recording functions.

A SCADA system comprises both hardware and software, and the classical SCADA system model includes the following components:

- Human-machine interface (HMI) – A program that provides the operator with an easy-to-read graphical and textual display of the SCADA system elements. The HMI displays warnings and alerts and supports the operator in analyzing system performance, spotting trends, and changing controls. Some commonly used HMI software packages are Wonderware, RSVIEW, and iFIX. An HMI is typically resident in the master control center as well as on the plant floor.
- Master terminal unit (MTU) or SCADA server at a master control center – A SCADA element at the control center that provides two-way data communication and control of field devices, such as RTUs, PLCs, PACs, and IEDs. Two-way communications between the MTU and field devices are usually low bandwidth and can be implemented through a variety of technologies, including telephone, VHF/UHF radio, spread-spectrum radio, satellite, and microwave.
- Remote terminal unit (RTU) – In a typical application, the RTU serves as a data concentrator and is an interface between the MTU and field devices, such as PLCs, PACs, or IEDs. The RTU gathers information from the field devices and stores it until interrogated by the MTU. Conversely, the RTU receives commands for the field devices and passes these on to be executed. There are some PLCs or PACs that incorporate the functions of the RTU by communicating with the MTU and providing remote data acquisition and control of field devices,

such as actuators and pumps.

- Programmable logic controller (PLC) – A PLC is defined as “a solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions, such as I/O control, logic, timing, counting, three-mode (PID) control, communication, arithmetic, and data and file processing.”³ A PLC uses a standard instruction set, such as IEC 61131-3, to implement control logic functions. IEC 61131-3 is a vendor-independent international standard for PLC programming languages for industrial automation. It includes standards for the following PLC programming languages:
 - Function block diagram (FBD)
 - Instruction list (IL)
 - Ladder diagram (LD)
 - Sequential function charts (SFC)
 - Structured text (ST)
- Programmable automation controller (PAC) – A PAC is similar to a PLC, but has additional capabilities, such as more robust communications, higher-speed processors, integration with organizational databases, and a common development environment for integration of software and hardware components.
- Intelligent electronic device (IED) – IED is a general term for a device that can communicate directly with the MTU or through the RTU and provide direct connections for controlling and polling field equipment, such as actuators.

Classical SCADA systems provide a dependable means of collecting information from multiple RTUs. However, in many current applications, SCADA systems are used in production environments and perform calculations and data analysis in real time on a plant floor, with HMI capabilities. Thus, in many instances SCADA and HMI reside on the same system to perform operations at the equipment level in a real-time data-driven production environment. The discussions in this book are meant to encompass both classical and current SCADA environments.

The SCADA control center serves as the central location for monitoring and analyzing data acquired from the field devices and for sending control commands to these devices. Because of its criticality, in many instances there is a duplicate control center at a backup site connected to the main site by a wide area network (WAN). Additional important capabilities that reside in the control center are archiving historical data, providing operations information

to business managers and accounting, and restoring lost data. This type of capability is usually provided by a data historian, a real-time relational database, and a yield accounting system.

The data historian acquires and stores data and provides for prompt recovery of that data, if required. It differs from a real-time database in that the historian only archives information and provides no outputs to other system devices. It offers additional capabilities, such as compressing data to store large amounts of data more efficiently and organizing the data into save-sets, which are histories of the system for specific time periods.

A real-time relational database supports interactive storage and retrieval of detailed contextual information when production processes are involved and can interface with business applications, other databases, forms, and XML files.

A yield accounting system interacts with the real-time relational database, processes plant production data, and generates production accounting information. Typical information provided by a yield accounting system includes:

- Inventory discrepancies
- Material balances in different areas of the plant and for the total plant
- Plant material movement
- Total amount of product made by a particular unit
- Total volume of a finished product shipped to a customer over a specified time interval

For planning and scheduling purposes, condensed versions of production data are transmitted from the yield accounting system to the enterprise resource planning (ERP) system for processing.

SCADA systems can be configured in a wide variety of architectures with various components, depending on the application and other plant and corporate requirements. [Figure 1-1](#) is an example of a SCADA system client-server model that incorporates fundamental SCADA elements. The figure is presented to provide a conceptual view of a SCADA system and is not intended to represent all the various SCADA system architectures that are employed in the field.

Distributed Control Systems

A DCS includes a supervisory controller running on a control server and a number of distributed controllers. The supervisory controller transmits data set points to the remote controllers and acquires data from them. The distributed controllers control process elements by communicating with them over a field-bus-type network based on the information received from the supervisor.

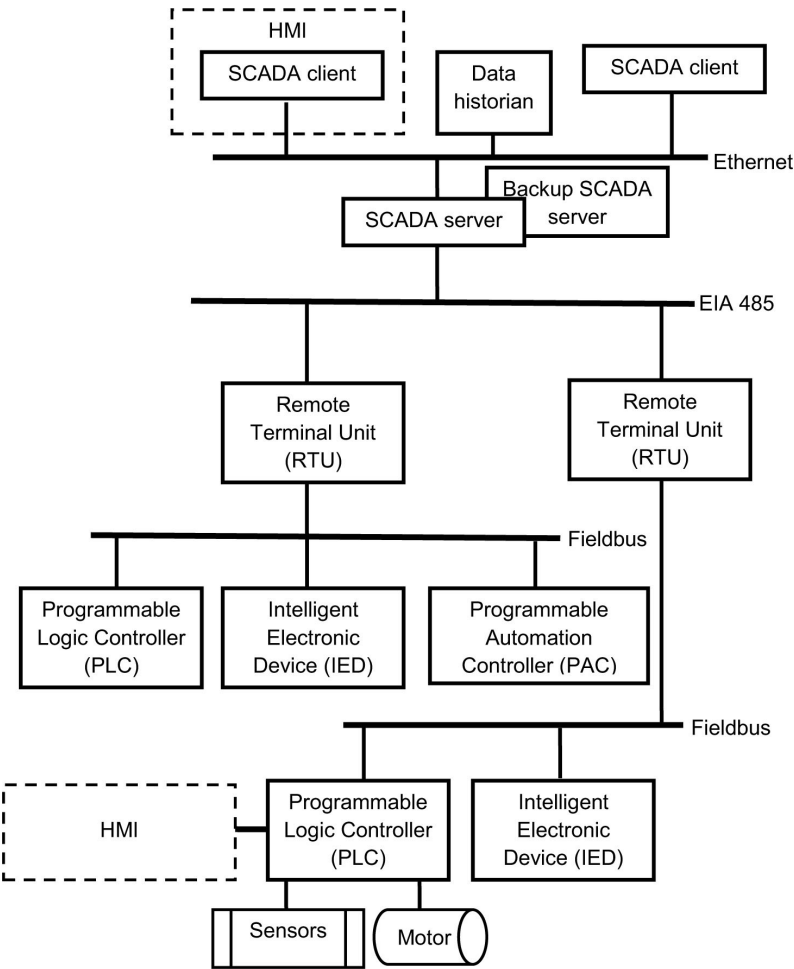


Figure 1-1. A client-server SCADA architecture example

ANSI/ISA-99.00.01-2007⁵ classifies a distributed control system as:

A type of control system in which the system elements are dispersed but operated in a coupled manner.

NOTE: Distributed control systems may have shorter coupling time constants than those typically found in SCADA systems.

NOTE: Distributed control systems are commonly associated with continuous processes, such as electric power generation, oil and gas refining, and chemical, pharmaceutical, and paper manufacture, as well as discrete processes such as automobile and other goods manufacture, packaging, and warehousing.

NIST 800-82⁶ defines a distributed control system as “control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit.”

In a distributed control system, subsystems have their own controller elements to manage local processes and to communicate with an operator console for overall supervisory functions. The individual controllers are integrated and communicate through local area networks. [Figure 1-2](#) illustrates a typical distributed control system. In the figure, the engineering workstation supports distributed system security functions, serves as a development facility, and is used to set alerts and alarm conditions. The operator workstation provides the operator interface and is used by the operator to monitor the distributed control system, sense alerts and critical situations, and conduct system diagnostics.

Safety Instrumented Systems

Safety instrumented systems (SISs) have been widely used in the process industry to maintain a process in a safe condition during a hazardous situation, for example, if critical set points are exceeded or safe operating conditions are breached. SISs are sometimes referred to as safety shutdown (SSD) systems or emergency shutdown (ESD) systems.

ANSI/ISA-84.00.01-2004, Part 1(IEC 61511-1 Mod)⁷ defines an SIS as an “instrumented system used to implement one or more safety instrumented functions (SIFs). An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).” The standard also defines an SIF as a “safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.” [Figure 1-3](#) illustrates the relationship between safety instrumented functions and other process functions.

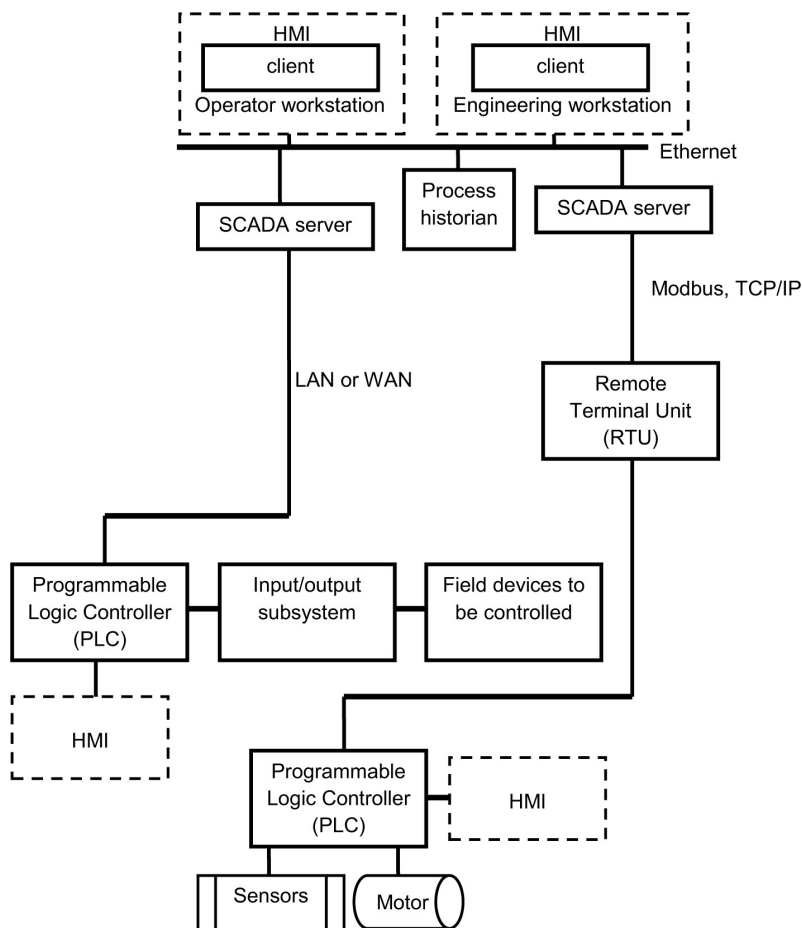


Figure 1-2. Example of a distributed control system

An SIS is usually implemented in parallel with conventional control systems to reduce the risks associated with explosive or other dangerous environments.

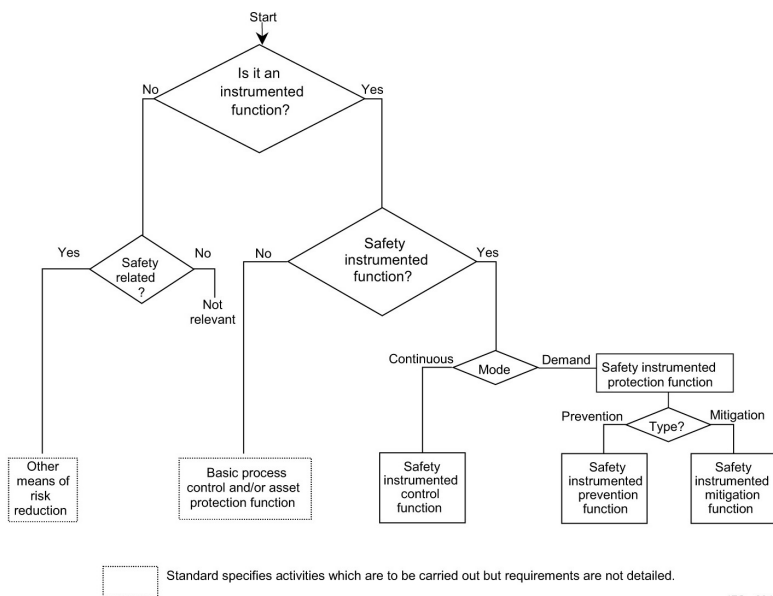


Figure 1-3. Safety instrumented functions vs. other process functions

[Source: ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod)]

Thus, the proper application of an SIS should be preceded by a formal risk assessment to identify possible threats, vulnerabilities, and likelihoods of occurrence. An excellent guide to risk management is NIST SP 800-39⁸, which takes a global, multitiered approach to risk management, where system risk is one part of a hierarchy of risk management levels. The document is aimed toward IT applications, but many of the principles are applicable to industrial automation and control systems. The document describes the following three tiers of an organization-wide risk management paradigm:

1. Tier 1 – Organization: Establishes and implements governance structures consistent with the organizational mission and goals.
2. Tier 2 – Mission/Business Processes: Designs, develops, and implements mission/business processes to support the mission defined in Tier 1.
3. Tier 3 – Information Systems: Integrates risk management activities into the system development life cycle (SDLC) of organizational information systems and addresses the resilience of organizational information systems.

NIST 800-39 will be discussed in more detail in [Chapter 5](#) of this book.

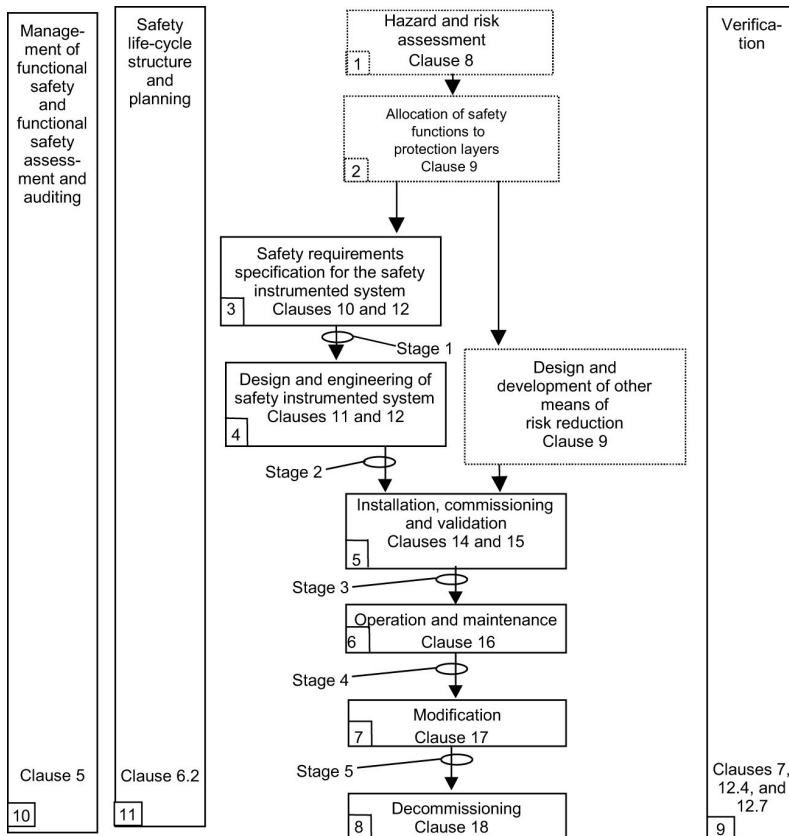
ANSI/ISA-84.00.01-2004 Part 1(IEC 61511-1 Mod) promotes two important concepts associated with an SIS, namely the safety life cycle and safety integrity levels, and defines these terms as follows:

- Safety life cycle – Necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use.
- Safety integrity level (SIL) – Discrete level (one of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented system. Safety integrity level 4 is the highest level of safety integrity; safety integrity level 1 is the lowest.

[Figure 1-4](#) provides a flow diagram of the SIS life cycle phases and functional safety assessment steps. The clauses cited in the figure refer to clauses in the ANSI/ISA-84.00.01-2004 document.

Industrial Automation and Control System Protocol Summary

A protocol defines the rules for entities to use in communicating with each other. In order to better manage communications and compartmentalize the activities required to establish, maintain, use, and close communication links, high-level models are used. In particular, layered architectures are useful in defining the various communication functions in a hierarchical manner. Two widely popular implementations of the layered architecture paradigm are the Open Systems Interconnect (OSI) model and the Transmission Control Protocol/Internet Protocol (TCP/IP) model.



NOTE 1 Stages 1 through 5 inclusive are defined in 5.2.6.1.3.

NOTE 2 All references are to Part 1 unless otherwise noted.

Figure 1-4. SIS life cycle and functional safety elements

[Source: ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod)]

The OSI Model

In the early 1980s, the International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) reference model. The model functions by encapsulating data and transferring it to an adjacent lower level, where the data is again encapsulated by the lower level, for example by adding a header. [Table 1-1](#) summarizes the OSI model layers and

Control)

NIST 800-82⁹ defines OPC as “a set of open standards developed to promote interoperability between disparate field devices, automation/control, and business systems.” The OPC standards specifications are now known as the Data Access Specification. OPC was built on the OLE COM (Component Object Model) and DCOM (Distributed Component Object Model) technologies of Microsoft, which specified a standard set of objects, interfaces, and methods for use in process control and manufacturing automation applications. Because of some vulnerabilities in Microsoft’s software, OPC should only be applied between the demilitarized zone (DMZ) and control networks and not used between the corporate network and the DMZ.

The following list summarizes some of the popular OPC specifications:

- OPC Alarms & Events – Supports process alarms, messaging, and event notifications on demand
- OPC Batch – Provides OPC functionality to batch processes
- OPC Command – Provides interfaces that support OPC clients and servers in managing commands sent to devices
- OPC Data Access – Provides for the transmission of data from PLCs, IEDs, and DCSs to HMI clients
- OPC Data eXchange – Supports interoperability among a variety of vendors and communication and management services among Ethernet fieldbus connections
- OPC Historical Data Access – Provides archiving of historical data
- OPC Security – Safeguards critical data through access control and integrity protection mechanisms
- OPC Unified Architecture – Defines specifications that do not use Microsoft COM in order to enhance cross-platform usage

OPC Unified Architecture

OPC Unified Architecture (OPC UA) is an OPC Foundation¹⁰ Web services technology designed to provide the functions of OPC, but to support interoperability among different platforms and achieve independence from Microsoft COM/DCOM. It can also interface easily with corporate enterprise systems and manufacturing management systems. Some of the features of OPC UA are:

- Integrated security
- Multiplatform compatibility
- Scalable

- Object-oriented
- Ability to identify specific components
- Information modeling, including how data is communicated

Modbus/TCP Model

Modbus is an OSI Layer 7 serial communication protocol that was developed by Modicon in 1979 for use with data acquisition and control systems. Modbus enables reliable communication among various control devices, including PLCs. A number of modifications to Modbus have evolved, such as Modbus/TCP, which was developed to be compatible with the TCP/IP model. Additional Modbus variants include Modbus ASCII, Modbus RTU, Modbus RTU/IP, and Modbus over UDP.

The DNP3 Protocol

The Distributed Network Protocol (DNP)3 is an open SCADA protocol that is used for serial or TCP/IP communications between control devices. It is widely used by utilities, such as water companies and electricity suppliers, for the exchange of data and control instructions between master control stations and remote computers or controllers called outstations. [Figure 1-5](#) is an example of a SCADA application, using DNP3 with a data concentrator in a hierarchical mode.

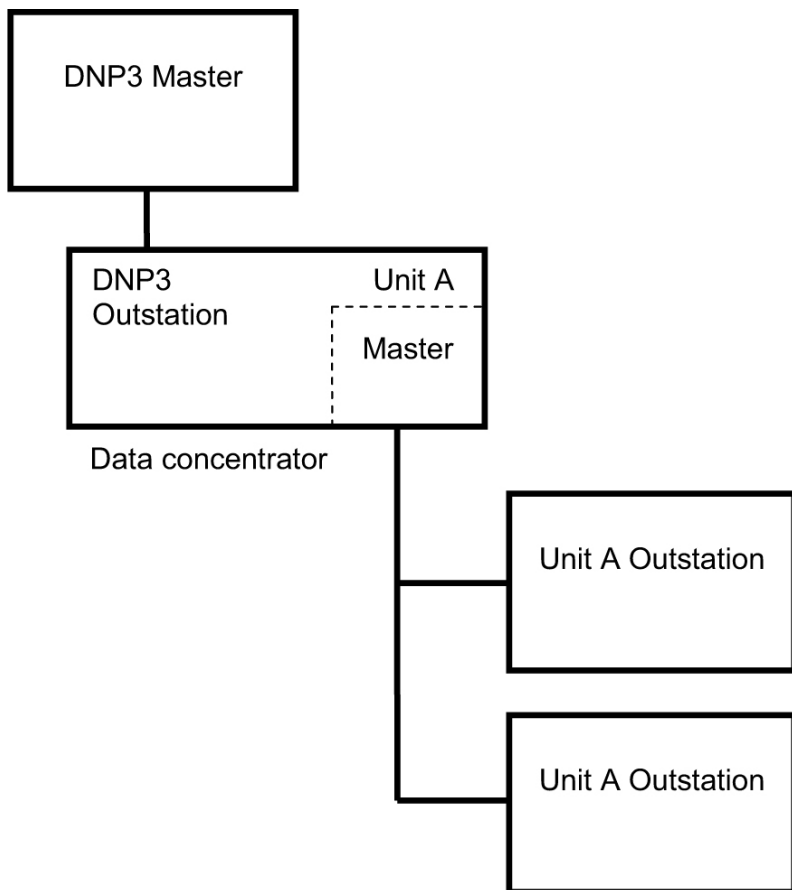


Figure 1-5. DNP3 example usage

Utility Communications Architecture 2.0/IEC61850

The Utility Communications Architecture (UCA), version 2.0, comprises a set of communications protocols for use by electric utilities. In 1999, UCA 2.0 evolved to the layered architecture standard IEC 61850 for substation automation. IEC 61850-enabled IEDs to obtain power grid condition data via an Ethernet process bus and from merge units, which provide interfaces to field devices. Legacy devices utilize an IEC 61850 wrapper around legacy protocols for compatibility. IEC 61850 includes the following features:

- Abstract definitions of services and data
- Definitions for IED communications
- IED communications through substation buses

- Mapping of services to protocols
- Object-oriented approach
- Standardized configuration language (SCL)

Figure 1-6 provides an overview of an IEC 61850-based substation.

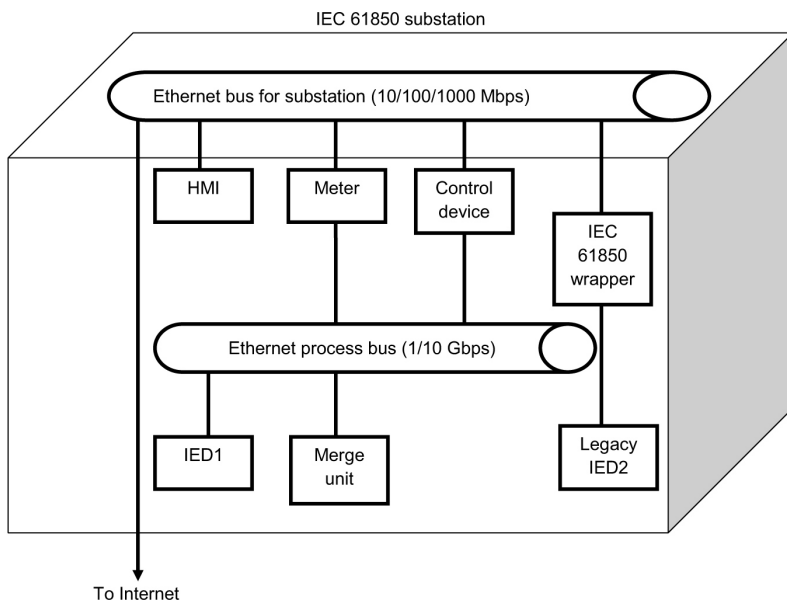


Figure 1-6. An IEC 61850 substation

Profibus

Process fieldbus or Profibus is an open standard that defines the electrical, mechanical, and functional aspects of a fieldbus that addresses deterministic data acquisition implementations. It is compatible with European international fieldbus standard EN 50 170. There are three versions of Profibus: Profibus Process Automation (PA), Profibus Decentralized Peripherals (DP), and Profibus Fieldbus Message Specification (FMS). Profibus PA communicates with control devices and data acquisition components through a common serial bus and is specifically designed for use in hazardous and explosive environments through current limiting elements. Profibus DP communicates over a high-speed network with sensors and actuators through a central controller and is suited for factory automation requirements. Profibus FMS supports communications among a large number of high-level applications at moderate transmission rates.

Controller Area Network

Controller Area Network (CAN) protocols, also known as ISO Standard 11898-1, were developed in 1986 by Robert Bosch GMBH in Germany for control applications in automobile production lines. The protocol uses an altered form of Ethernet Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to implement a deterministic protocol for SCADA systems. In a deterministic system, an element must respond to events in a predictable manner with a known response time. For example, when controlling a robot arm, its position must be known, and the time it takes to obtain position information must be within certain bounds. Similarly, the time it takes to send commands to the arm and have it respond must be predictable and bounded.

EtherNet/IP

EtherNet/IP is an application layer protocol designed for industrial automation and control systems applications and is a member of a family of networks that implement the Common Industrial Protocol (CIP) at its upper layers. EtherNet/IP provides control, configuration, and data exchange capabilities on an Ethernet network. The protocol defines network entities and devices as objects and uses a TCP/IP object for the TCP/IP protocol and an Ethernet link object to set up an EtherNet/IP link. EtherNet/IP uses the Open Systems Interconnection (OSI) model and implements CIP at the session layer and above, and adapts CIP to the specific Ethernet/IP technology at the Transport layer and the lower layers. A typical EtherNet/IP architecture is shown in [Figure 1-7](#).

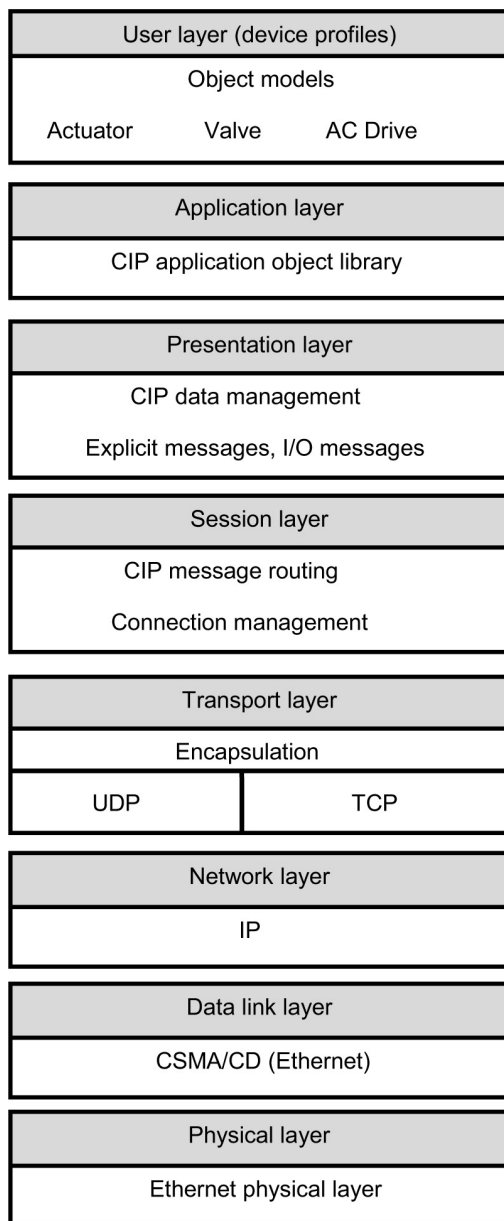


Figure 1-7. A typical EtherNet/IP architecture

openSAFETY Protocol

OpenSAFETY¹¹ is an application layer protocol sponsored by the Ethernet Powerlink Standardization Group¹² (EPSC), which supports the

communication of safety-related data over a variety of industrial networks and ensures data transfer integrity. The performance of openSAFETY data communications is a function of the network and the specific data transfer protocols being used. For example, openSAFETY can be used with Modbus and EtherNet/IP. It is compatible with IEC 61508 and can provide safe implementations up to SIL-3. An important characteristic of openSAFETY is that it employs a variable-length frame with a uniform format that supports safe distribution of values. To meet these requirements, openSAFETY verifies parameters using cyclic redundancy check (CRC) and encapsulates its messages, which independently tunnel through the extant protocols being used in the data acquisition and control network. [Figure 1-8](#) illustrates the relationship of openSAFETY to the other protocols in the OSI layered architecture.

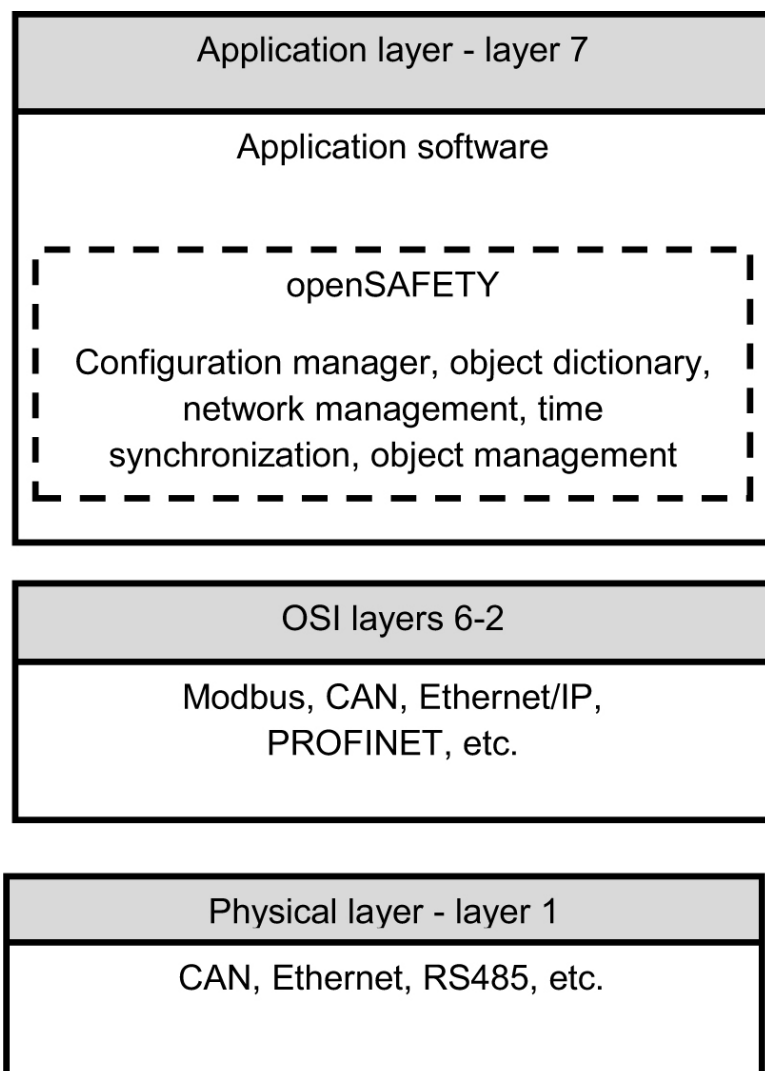


Figure 1-8. A typical openSAFETY architecture

Issues in Industrial Automation and Control Systems Security

No one questions the need to protect a nation's critical infrastructure and essential production processes. The available means and methods required to accomplish this defense are varied and have multiple characteristics associated with them. These characteristics include:

- Hardware cost
- Software cost
- Reliability
- Level of assurance
- The effect of security controls on performance
- Maintenance issues
- Safety issues
- Effect on product quality
- Response to emergency situations
- Interfaces to management systems
- Compatibility with 24/7 operations

These issues and others will be explored in the chapters of this book to provide a foundation for securing industrial automation and control systems.

Summary

Over the past two decades, methodologies and best practices in the field of information system security have been developed, refined, and codified. They comprise a rich compendium of proven and effective measures to secure computer systems and networks. The fundamentals of these developments will be presented in [Chapter 2](#) as a basis for the evolution of security technologies applicable to industrial automation and control systems. A number of these paradigms are not directly applicable to industrial automation and control systems, but many are, and many can be employed with modifications tailored to the unique characteristics of these systems. These adapted methods can be effective in securing industrial automation and control systems against threats, such as viruses, Trojan horses, worms, and attacks that result in the unauthorized modification and manipulation of critical data, denial of service and availability, unauthorized modification of audit logs, and general disruption of critical operations.

The information system security approaches embrace a wide variety of disciplines and include:

- Policies, procedures, and standards
- Access control mechanisms

- Physical security
- Identification and authentication technologies, such as biometrics and security tokens
- Audit trails
- Real-time monitoring of system and network information
- Risk management
- Business continuity and disaster recovery planning
- Firewalls to filter message traffic
- Intrusion detection and protection systems
- Public key and secret key cryptography
- Malware detection, isolation, and elimination

Review Questions for Chapter 1

(Please read the questions carefully and select the one BEST answer.)

1. According to NIST SP 800-82, the term “industrial control system” encompasses which of the following?
 - a. SCADA systems
 - b. Distributed control systems (DCSs)
 - c. Programmable logic controllers (PLCs)
 - d. All of the above

2. According to ANSI/ISA-99.00.01, “a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process” is a(n):
 - a. Industrial automation and control system
 - b. Distributed control system
 - c. Discrete control system
 - d. Programmable logic controller

3. A “type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems” is

defined by ANSI/ISA-99.00.01 as which of the following?

- a.Distributed control system
- b.SCADA system
- c.Safety instrumented system (SIS)
- d.Human-machine interface (HMI)

4.Which one of the following items is NOT a component of a classical SCADA system model?

- a.Human-machine interface (HMI)
- b.Remote terminal unit (RTU)
- c.Enterprise resource planning (ERP)
- d.Programmable logic controller (PLC)

5.Which of the following is NOT a characteristic of a SCADA master terminal unit (MTU)?

- a.Has two-way communication with field devices
- b.Usually located at the master control center
- c.Has high-bandwidth communication requirements
- d.Communicates through telephone, VHF/UHF radio, spread spectrum radio, satellite, and/or microwave

6.In a typical SCADA application, what component serves as a data concentrator and is an interface between the MTU and field devices?

- a.HMI
- b.RTU
- c.Data historian
- d.Relational database

7.IEC standard 61131-3 was designed to make it easier to implement control logic functions. IEC 61131-3 is which of the following?

- a.Vendor-independent international standard for PLC programming languages
- b.Standard guide to industrial control systems
- c.Safety instrumented systems (SIS) standard for the process

industry

d.Integrated enterprise-wide risk management standard

8.Which of the following is NOT a characteristic of a data historian?

a.Provides for prompt recovery of data

b.Performs data compression

c.Supports interactive storage and retrieval of detailed production information

d.Provides system histories over given time periods

9.A yield accounting system used in conjunction with a SCADA system provides which of the following functions?

a.Plant material movement

b.Inventory discrepancies

c.Material balances

d.All of the above

10.ANSI/ISA-99.00.01-2007 defines which of the following as “a type of control system in which the system elements are dispersed but operated in a coupled manner?”

a.Distributed control system

b.Discrete control system

c.Dispersed control system

d.Coupled control system

11.ANSI/ISA-84.00.01-2004 Part 1(IEC 61511-1 Mod) defines which of the following as an “instrumented system used to implement one or more safety instrumented functions (SIF)”?

a.Safety surety system

b.Failure proof system

c.Safety instrumented system

d.Safety function system

12.Necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept

phase of a project and finishes when all of the safety instrumented functions are no longer available for use is known as which of the following?

- a.Safety duration
- b.Safety life cycle
- c.Safety boundary
- d.Safety period

13.The safety integrity level (SIL) is a discrete level for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Which of the following statements is TRUE?

- a.Safety integrity level 4 has the lowest level of safety integrity; safety integrity level 1 has the highest.
- b.Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.
- c.Safety integrity level 3 has the highest level of safety integrity; safety integrity level 1 has the lowest.
- d.Safety integrity level 3 has the lowest level of safety integrity; safety integrity level 1 has the highest.

14.The Open Systems Interconnection (OSI) reference model has how many layers?

- a.Six
- b.Five
- c.Seven
- d.Four

15.Which layer of the OSI model converts packets into electrical or optical signals for sending on the transmission media?

- a.Application
- b.Presentation
- c.Physical
- d.Session

16.What are the four layers of the TCP/IP model?

- a.Application, Host-to-Host, Internet, and Network Access
- b.Application, Presentation, Internet, and Network Access
- c.Application, Network, Internet, and Network Access
- d.Application, Host-to-Host, Internet, and Physical

17.NIST 800-82 defines which of the following as “a set of open standards developed to promote interoperability between disparate field devices, automation/control, and business systems”?

- a.Modbus/TCP
- b.OPC
- c.DNP3
- d.Profibus

18.The protocol that supports the communication of safety-related data over a variety of industrial networks and ensures data transfer integrity is known as which of the following?

- a.Safety instrumented system (SIS)
- b.Safety instrumented function (SIF)
- c.OpenSAFETY
- d.ClosedSafety

19.Which of the following statements relative to the IEC layered architecture Standard IEC 61850 for substation automation is NOT true?

- a.It is a set of protocols for electric utilities.
- b.IEC-enabled devices can obtain power grid condition data via an Ethernet process bus.
- c.Merge units provide interfaces to field devices.
- d.It is not compatible with legacy protocols.

20.Which of the following are versions of Profibus?

- a.Profibus PA, Profibus CP, Profibus CIP
- b.Profibus PA, Profibus DP, Profibus FMS
- c.Profibus PA, Profibus CP, Profibus FMS
- d.Profibus PA, Profibus CIP, Profibus FMS

References

- 1 ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, October 2007.
- 2 NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other control system configurations, such as Programmable Logic Controllers (PLC)*, Final Public Draft, September 2008.
- 3 IEEE Std. C37.1-1994, *IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control*, Institute of Electrical and Electronics Engineers, 1994.
- 4 *The Automation, Systems, and Instrumentation Dictionary*, 4th Edition. Research Triangle Park: ISA, 2003.
- 5 ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, October 2007.
- 6 NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other control system configurations, such as Programmable Logic Controllers (PLC)*, Final Public Draft, September 2008.
- 7 ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*, September 2004.
- 8 NIST Special Publication 800-39, *Integrated Enterprise-Wide Risk Management Organization, Mission, and Information System View*, Final Public Draft, December 2010.
- 9 NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*, Final Public Draft, September 2008.
- 10 <http://www.opcfoundation.org/>
- 11 <http://www.open-safety.com>
- 12 <http://www.ethernet-powerlink.org/index.php?id=43>

Chapter 2

Information System Security Technology

Chapter 1 provided a review of some fundamental industrial automation and control system concepts, assuming that the reader has some familiarity with these systems. Because this book is focused on the security of industrial automation and control systems, *Chapter 2* will delve into the details of information system security in order to provide a basis for developing effective security approaches for industrial automation and control systems. The field of information system security has evolved over decades and is an abundant source of valuable knowledge and techniques that have been proven over time. By taking into account the unique characteristics of industrial automation and control systems, the technology of information system security can be adapted and tailored to provide effective security for the many types of industrial automation and control applications.

Information System Security Fundamentals

Information system security is defined as comprising the three basic elements of confidentiality, integrity, and availability, or C-I-A. These three concepts form the C-I-A triad, as shown in [Figure 2-1](#).

Additional complementary elements that support information system security are identification, authentication, authorization, accountability, auditing, and nonrepudiation. These important topics are summarized in the following sections.

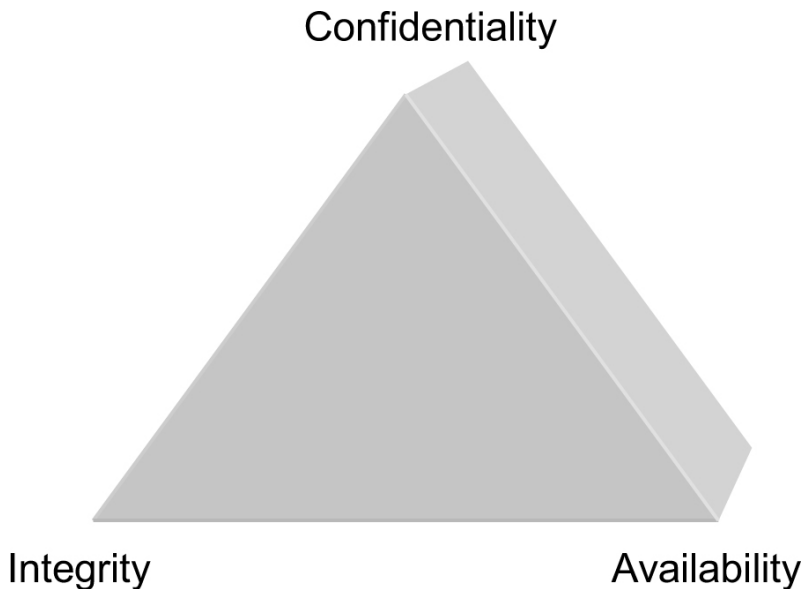


Figure 2-1. The C-I-A triad

Confidentiality

Confidentiality refers to protecting documents, messages, computer files, and so on from being disclosed, either intentionally or unintentionally, in an unauthorized manner. Examples of loss of confidentiality are an unauthorized individual intercepting and reading a message sent across a network or the revelation of a company's trade secret. Confidentiality is related to privacy of information in that it is concerned with the unauthorized disclosure of sensitive information.

Integrity

Integrity (as applied to data) is concerned with the unauthorized modification of data, whether by an authorized or an unauthorized individual or process. If a message is intercepted, its contents are changed, and it is then forwarded to a receiver, its integrity has been violated.

Availability

Availability is a measure of the ability of an authorized person or process to have prompt and reliable access to computational resources when needed. For example, availability would be compromised if an individual is prevented from conducting an online financial transaction because the financial organization's Web site is down.

Identification

Identification is the act of professing an identity to a system or process. A typical example of identification is a computer user typing in a user ID when logging onto a computer system.

Authentication

Authentication is the act of verifying an identity and confirming that an entity is what it professes to be. An example of authentication is verifying that a logon user ID actually belongs to the claimed user.

Authorization

When identification and authentication are completed, a user or process can be granted access privileges to specific computer information or resources. Different individuals or processes can be granted different levels of authorization, depending on the sensitivity of the information being accessed and the level of the rights granted to those individuals or processes to access the information.

Accountability

Accountability is the ability to identify an individual and to hold that individual responsible for his or her actions. Tools, such as audit logs, can help in determining accountability and uncover activities that were conducted by individuals or processes.

Auditing

Auditing is the act of reviewing logs or records at specified intervals to determine if violations of system security have occurred. Typical audit logs include information such as where and when a transaction occurred and who conducted the transaction. Information technology auditors can either be internal auditors, working for the organization under audit, or external auditors, belonging to an outside organization. A companion endeavor to auditing is monitoring, which refers to a continuing activity, such as intrusion detection on a network or host computer.

Nonrepudiation

Nonrepudiation in digital systems refers to ensuring that the sender of a message or contract cannot later deny sending the message or contract and that, conversely, a receiver to whom the message was sent cannot deny receiving the message. Digital signatures are used to implement nonrepudiation in electronic transactions, and they will be discussed later in this chapter.

Related Terminology

In addition to the above principles, four related terms that appear throughout

the information security landscape and that should be understood by all involved with protecting computer systems and networks are:

- Asset – An organization’s important resource, whose loss or compromise could negatively impact confidentiality, integrity, or availability and could also result in financial loss. Therefore, an asset should be protected from attack or compromise.
- Threat – As defined by NIST SP 800-53¹: “Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.”
- Safeguard – A security control or countermeasure designed to mitigate the risk associated with a specific threat or group of threats.
- Vulnerability – The absence or weakness of a safeguard. According to NIST 800-53, vulnerability is “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.”

Vulnerability can be decreased by applying controls that will mitigate the effect of an attack. Controls can be partitioned into the following categories:

- Corrective controls minimize the effect of an attack and the degree of resulting damage.
- Detective controls discern if attacks have occurred or are occurring, and initiate control measures.
- Deterrent controls reduce the potential for an attack to occur.
- Preventive controls prevent a threat from exploiting a vulnerability.

One means that is used to prioritize which controls to apply and where to apply them is a threat matrix. The threat matrix plots the impact an attack would have if it is successful versus the likelihood that the attack will occur. In this way, resources can be applied to mitigate the threats with the highest impact and the highest likelihood of occurrence. The objective of this activity is to move all threats into the low impact and low likelihood of occurrence area, as shown in [Figure 2-2](#).

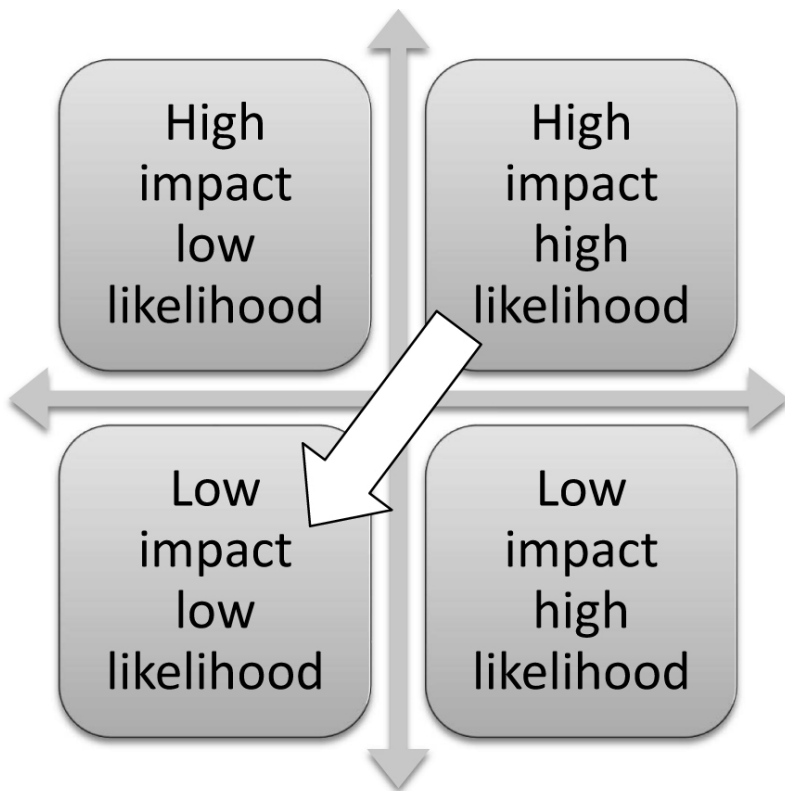


Figure 2-2. A threat matrix

NIST SP 800-53 provides a comprehensive list of recommended security controls.

Types and Classes of Attack

The Information Assurance Technical Framework (IATF) document 3.1,² sponsored by the National Security Agency (NSA), identifies the following types of attacks:

- Passive
- Active
- Close-in
- Insider

- Distribution

These attacks and their description are summarized in [Table 2-1](#).

Table 2-1. Types of Attacks

Definition
Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capture of authentication information (such as passwords). Passive attacks can result in disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.
Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These attacks may be mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. (An enclave is collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.) Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.
Close-In attack consists of individuals, not normally insiders, attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry, open access, or both.
Insider attacks can be malicious or nonmalicious. Malicious insiders intentionally eavesdrop, steal, or damage information, use information in a fraudulent manner, or deny access to other authorized users. Non-malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as “getting the job done.”
Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code into a product, such as a back door to gain unauthorized access to information or a system function at a later date.

[Source: IATF Document 3.1, September 2002.]

Additional System Security Concepts

In industrial automation and control systems as well as in information technology systems, it is important that the computer resources, networks, and associated equipment operate reliably, efficiently, and securely in performing the actions for which they were designed. A number of useful principles for designing and implementing secure IT systems have evolved and are important tools that can be applied to industrial automation and control systems. The following principles were delineated in a 1974 paper by Saltzer and Schroeder³:

- Complete Mediation
- Defense in Depth

- Economy of Mechanism
- Fail Safe
- Least Common Mechanism
- Least Privilege
- Leveraging Existing Components
- Open Design
- Psychological Acceptability
- Separation of Duties
- Weakest Link

The fundamental characteristics of these principles are summarized as follows:

Complete Mediation

Complete mediation requires that when an entity (a user or process) requests access to an object, such as a file or document in a computer system, the entity must go through a valid authorization process that cannot be circumvented.

Defense in Depth

Defense in depth is the act of establishing numerous layers of protection wherein a subsequent layer will provide protection if a previous layer is breached. NIST Special Publication 800-82⁴ defines a defense-in-depth architecture strategy as “the use of firewalls, the creation of demilitarized zones, and intrusion detection capabilities, along with effective security policies, training programs, and incident response mechanisms.” ANSI/ISA-99.00.01⁵ describes defense in depth as:

Provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack.

NOTE: Defense in depth implies layers of security and detection, even on single systems, and provides the following features:

Attackers are faced with breaking through or bypassing each layer without being detected.

A flaw in one layer can be mitigated by capabilities in

other layers.

System security becomes a set of layers within the overall network security.

Economy of Mechanism

Economy of mechanism advances the concept that the design and implementation of defensive mechanisms should be straightforward, understandable, and not unnecessarily complex. Following these guidelines makes it easier to detect possible unauthorized access routes into the information system that could be used to acquire sensitive data or launch an attack.

Fail Safe

NIST SP 800-123⁶ explains the term *fail safe* as “If a failure occurs, the system should fail in a secure manner, i.e., security controls and settings remain in effect and are enforced. It is usually better to lose functionality rather than security.” Also, a fail-safe design should ensure that when a system recovers from a failure, it should recover in a secure state, where only authorized users have access to sensitive information.

Least Common Mechanism

Least common mechanism refers to having the least possible sharing of common security mechanisms among users or processes. Having many users sharing common security mechanisms can result in unknown or unauthorized access paths to sensitive data.

Least Privilege

In the principle of least privilege, a user or process is given the minimum amount of privileges, authorization, and so on, for the smallest amount of time that will permit the user or process to accomplish assigned tasks. Least privilege reduces the prospect of an individual or process having unauthorized access to sensitive information.

Leveraging Existing Components

Leveraging existing components is using the security mechanisms that are already in place in the most efficient and effective manner and to their maximum capabilities. This process can be accomplished by periodically reviewing the configuration of the security devices and optimizing their operational performance.

Open Design

Open design proposes that making designs and security approaches available to examination and scrutiny by a variety of parties will ensure that they are

robust and are performing as required. The concept is that by making the designs available for review, any flaws or weaknesses can be exposed and corrected. The alternative to open design is to keep designs proprietary and confidential in the hope that by doing so they will be more secure from compromise. In almost all cases, open design results in more effective and reliable mechanisms.

Psychological Acceptability

Psychological acceptability is concerned with making the interface and interaction with access control mechanisms intuitive and easy for the user to understand and operate. In this way, the security controls will not be seen as interfering with the tasks at hand and as an obstacle to getting things done.

Separation of Duties

Separation of duties requires that functions, roles, or responsibilities should be distinct and independent from each other so that no entity can solely control sensitive operations. An example is that a person requesting or ordering an expensive item should not be the same person that signs the check for its purchase. Separation of duties forces multiple individuals to collude if they are going to commit fraud or obtain unauthorized access to data.

Weakest Link

As with any group of protection mechanisms, it is important to identify the weakest element in the group. Once the weakest link is identified, actions can be taken to bolster that element and mitigate any corresponding risk.

Policies, Standards, Guidelines, and Procedures

In addition to secure design principles, documents professing management's view of security and describing techniques of implementation are valuable tools in establishing the security of an organization. Four important categories of such tools are policies, standards, guidelines, and procedures.

Policies

In general terms, a policy is a statement of the intent of management for the organization, and compliance is mandatory. A policy is an important document because it provides top-down requirements for the organization and is necessary to protect sensitive information, prevent liability issues, and meet regulatory and legal requirements.

NIST SP 800-127 defines the following three types of computer system security policies:

- Program policy – Creates an organization’s computer security program
- Issue-specific policies – Addresses specific issues of concern to the organization
- System-specific policies – Protects a particular system through technical directives set forth by management

Table 2-2 summarizes the characteristics of the NIST policy types.

Table 2-2. NIST Policy Types

Policy Type	Description
High-level program policy	Establishes the organization's security posture and intent
Issue-specific policy	Addresses specific security issues
System-specific policy	Establishes specific controls for a particular system

[Source: NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*]

Standards

A standard details how specific methods must be applied in a consistent manner. For example, a standard for the types of information security controls that must be applied would ensure that all elements of the organization are incorporating technologies in a uniform manner. Conformance to standards is normally compulsory.

Guidelines

Guidelines also detail methods to use to create secure information systems, but are considered to be recommendations and conformance is not compulsory.

Procedures

Procedures are step-by-step actions that must be taken to implement policies and standards. Procedures describe compulsory activities.

Malicious Code and Attacks

NIST SP 800-538 defines malicious code as:

Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an

information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malicious code (malware) is used in attacks against information systems and industrial automation and control systems. Some of the main types of attacks are reviewed in the following sections.

Viruses and Worms

ANSI/ISA-99.00.01-2007⁹ defines a virus as a “self-replicating or self-reproducing program that spreads by inserting copies of itself into other executable code or documents,” and a worm as a “computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network and may consume computer resources destructively.” Note that a worm does not require other executable software to propagate but can move across networks to infect other hosts on its own.

Trojan Horse

A Trojan horse conceals additional code in a program that is used for a valid purpose. Then, the hidden code, which could be a virus, can perform malicious acts. Trojan horses can be transmitted through emails or downloads from Web sites.

Logic Bomb

A logic bomb is a type of Trojan horse that does not execute until a preset condition is met, for example, at a specific time and date or when some activity is performed on the host computer.

Mobile Code

Software that is obtained or downloaded over a network from a remote source onto a local computer is known as mobile code. This mobile code can be used for valid applications or can contain a virus that could do harm to a computer system.

Back Door

In a back door attack, an individual attempts to gain access to a computer system by circumventing its protection mechanisms. An example is using a dial-up modem to call into a person's desktop computer and then accessing the organization's network through that computer.

Scanning

In scanning, an individual can locally or remotely connect to a computing system and obtain information about that system that can be used later in

launching an attack. A scan can yield the following information:

- Open ports
- Services that are running
- Types of system software
- Domain names
- Existence of intrusion detection systems
- Protocols being used
- Existence of firewalls and perimeter devices

If a system is being scanned, this activity should be viewed as a prelude to a possible attack.

Man-in-the-Middle

A man-in-the-middle (MitM) attack focuses on the authentication protocol between a claiming party and a verifying party communicating with each other. For example, a claiming party can be asked to present and transmit particular credentials while the verifying party receives those credentials. In a successful attack, the attacker can intercept data between the two parties, modify it, and then pass it on without the knowledge of the sender or receiver.

Social Engineering

Social engineering uses “soft” methods to acquire sensitive information. Social engineering methods may be used to deceive individuals into revealing sensitive information, such as passwords or PIN numbers. Persuasive phone calls to an individual from an attacker impersonating someone in a position of authority, a phony email, or a fake call pretending to be from a help desk can elicit private information that can be used later against the organization. Social engineering threats can be minimized through effective awareness training and security policies.

Guessing Passwords

An attacker can use a variety of means to determine a user’s password to gain entry to a computer system. Guessing, searching an area for passwords written on post-it notes, and looking over someone’s shoulder are all methods that can be used to determine passwords. One approach, known as a dictionary attack, uses a dictionary of commonly used passwords to try to gain entry to a system.

Denial of Service/Distributed Denial of Service

A denial of service (DoS) attack is one that is designed to overwhelm a computer system's resources to the point where it can no longer perform its required functions. Thus, a DoS incident affects the availability of the computer system. In distributed denial of service (DDoS), the attacks on availability originate from multiple sources that work in concert to saturate a computer system's capabilities. In many instances, these sources are host computers on which the malicious DDoS software has been installed without the owner's knowledge.

Replay

In a replay attack, the perpetrator intercepts a message and saves it to be sent at a later time, when it seems to come from the original sender. A countermeasure to this attack is to attach a timestamp to the message at the time it was sent. Then, if the message is intercepted and sent at a later time, the timestamp will show it is an old message.

Dumpster Diving

In dumpster diving, an individual sorts through discarded material in a dumpster in hope of finding sensitive information that can be used later to attack an organization's computer system. In many cases, user's manuals, technical manuals, correspondence, organization charts, and other related material can provide valuable information to an attacker.

Firewalls

One of the important defenses against malware is a properly configured and implemented firewall. Firewalls implemented in industrial automation and control systems have to be "aware" of the special requirements and characteristics of such systems. The major types of firewalls are discussed in this section. NIST SP 800-41 [10](#) defines firewalls as "devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures." ANSI/ISA-99.00.01-2007 describes a firewall as:

an internetwork connection device that restricts data communication traffic between two connected networks.

NOTE: A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

Firewalls are categorized as to their technical implementation and their architecture. The technical categories are packet filtering, stateful inspection, application, and application proxy. The architectural categories are screened-host, dual-homed host, and screened subnet firewall. These categories are reviewed in the following sections.

Packet Filtering Firewall

A packet filtering firewall resides at the network layer of the OSI model and determines which packets can be allowed to continue to their destination addresses by inspecting the packet source and destination addresses. It filters the packets based on firewall access control lists (ACLs), which specify the packets that can be sent to particular destination addresses or to specific application port destinations. [Figure 2-3](#) illustrates a packet filtering firewall.

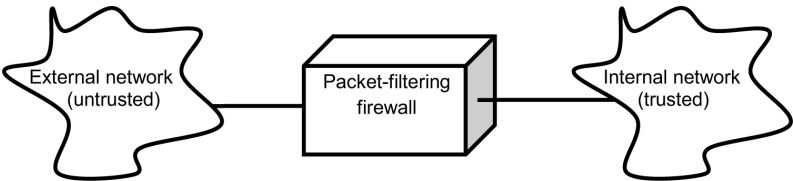


Figure 2-3. A packet filtering firewall

Stateful Inspection

A stateful inspection firewall improves on a packet filtering firewall by determining the state of incoming data connections at the network layer and blocking data packets that do not conform to the anticipated state. A state refers to one of the three primary states associated with TCP communications, namely, initiating the connection, establishing and using the connection, and terminating the connection. This information is contained in TCP headers and can indicate if a packet is not in its proper state. An attacker might place information in the header, indicating that the packet is in one state when it is actually in another. In this instance, the packet will not be passed through the firewall.

In addition to state information, the packet header also includes the source IP address, destination IP address, and port numbers. This information is stored in a dynamic state table for processing. An example of a state table is shown in [Table 2-3](#).

Table 2-3. Example State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established
[Source: NIST SP 800-41 Revision 1, <i>Guidelines on Firewalls and Firewall Policy</i> , September 2009.]				

As an example of the firewall use of the state table, the source address (192.168.1.100) in the first row of the state table is an internal address behind the firewall and is initiating a connection to an IP address (192.0.2.71) outside of the firewall. This connection would have to be allowed under the firewall security policy.

Application Firewall

An application firewall performs what is sometimes referred to as deep packet inspection by incorporating stateful protocol analysis. This analysis is performed at the application layer of the OSI model and compares stored profiles of normal protocol usage against actual usage that might indicate malicious activity in an application. If malicious activity is detected, the firewall could inhibit specific connections to the information system. Potential malicious activity could include email with harmful attachments, unexpected command sequences, and the downloading of active mobile code.

Application-Proxy Gateway

An application-proxy gateway firewall serves as an intermediary between networks and serves to mask the source of a message. The application-proxy gateway operates at the application layer of the OSI model and provides a higher level of security at the expense of additional time being required for processing the data.

This type of firewall can be implemented by executing proxy software on a workstation that masks an internal network from external entities attempting to gain information about that network. Thus, the connection consists of communication between an internal computer and the proxy server and a connection between the proxy server and an external network. Most application proxy firewalls operate with HTTP. [Figure 2-4](#) is an example of an application-proxy gateway.

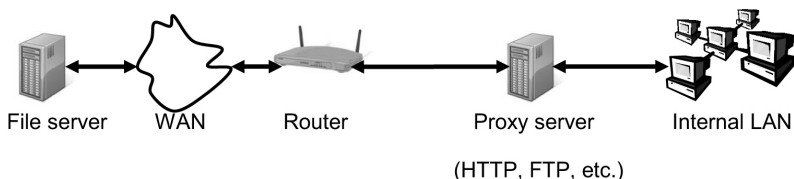


Figure 2-4. Application-proxy gateway

Screened-Host Firewall

A screened-host firewall uses a host to connect two networks together. This connection is accomplished through two network interface cards (NICs) that respectively connect to each one of the networks, with a screening router between the host and the untrusted network. This arrangement offers both proxy and routing capabilities. In this architecture, the firewall is facing outward toward the untrusted network and serves to protect the host and the trusted network. [Figure 2-5](#) illustrates a screened-host firewall.

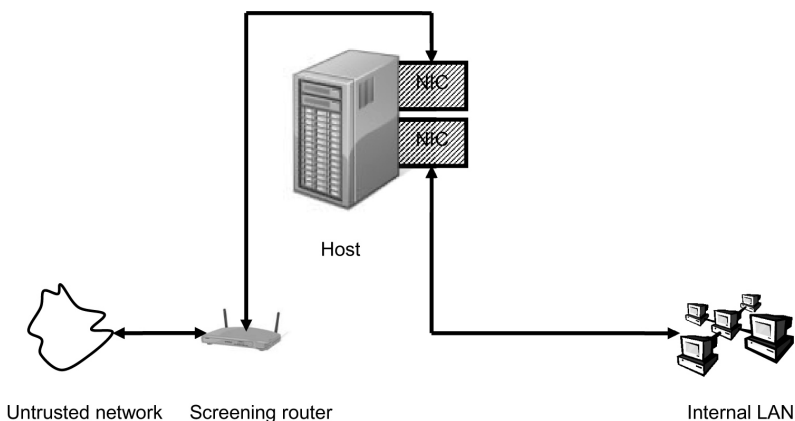


Figure 2-5. Screened-host firewall

Dual-Homed Host Firewalls

An architecture similar to the screened-host firewall is the dual-homed host firewall. In this configuration, a host with two NICs connects a trusted network to an untrusted network, but does not employ a screening router. The host acts as a filter to packets passing between the networks and is configured as a strong defense against attacks. This type of host is known as a bastion host. [Figure 2-6](#) shows a dual-homed host firewall configuration.

Screened-Subnet Firewalls

A screened-subnet firewall employs another variation of two NICs with a bastion host. It uses packet filtering routers on the trusted and untrusted network sides, and the host provides proxy services. The screened-subnet architecture also defines a demilitarized zone (DMZ) or perimeter network, which is a third network that lies between the internal trusted network and the external untrusted network as an added layer of protection. [Figure 2-7](#) is an example of a screened-subnet firewall.

Additional means to protect information systems include scrambling the data so that it cannot be read or compromised by an attacker. This approach employs cryptography, which will be discussed in the next section.

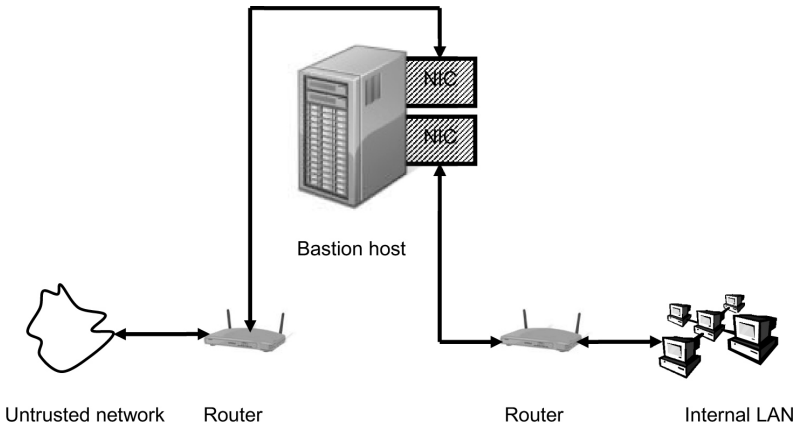


Figure 2-6. Dual-homed host firewall

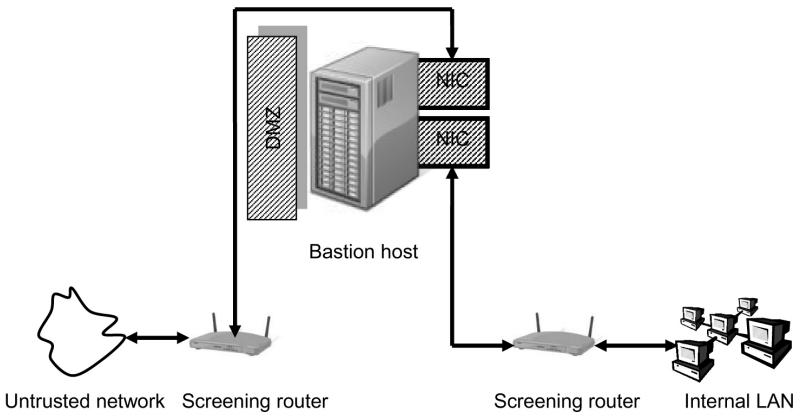


Figure 2-7. Screened-subnet firewall

Cryptography

The purpose of cryptography is to protect transmitted information from being read and understood by anyone except the intended recipient. Cryptography can be used to implement confidentiality, integrity, authentication, and non-repudiation.

The most familiar form of cryptography is secret key or symmetric key cryptography, where the sender and receiver both know a secret key. The sender encrypts a plaintext message with the secret key, and the receiver decrypts the message with the secret key. Thus, the sender and receiver have a shared secret. One of the problems with secret key cryptography is how to securely distribute the secret key used by the sender to the receiver. This distribution might be accomplished with a messenger or by another out-of-band communication means, such as by fax or mail. Out-of-band communications refer to using another means of communication that is different from the means used to send the main message.

A solution to the key distribution problem of secret key encryption came in the development of asymmetric or public key encryption. In asymmetric key cryptography, the receiver holds a private key, and the sender uses a public key to encrypt the message. The public and private keys are related mathematically such that a message encrypted with the public key can be decrypted only with the private key held by the receiver. The public key is made available to anyone who wants to use it, and the private key of the pair is held secret by the receiver. The private and public keys are related, but in the ideal case, they share the characteristic that the private key cannot be derived using knowledge about the public key.

Public key cryptography requires more computations than secret key cryptography and is therefore much slower in data transmission than secret key cryptography. Symmetric and asymmetric key cryptography are discussed in more detail in the following sections.

Symmetric Key Cryptography

In symmetric key cryptography, it is critical that the secret key be kept secure and uncompromised. In an ideal situation, a secret key would be used only once and would not be used in subsequent transmissions. In general, the symmetric key encryption algorithm is known and is available to the public, but the cryptographic system is secure if the secret key or cryptovariable, as it is sometimes called, is kept private and secure. A symmetric key cryptographic system (“cryptosystem”) block diagram is shown in [Figure 2-8](#).

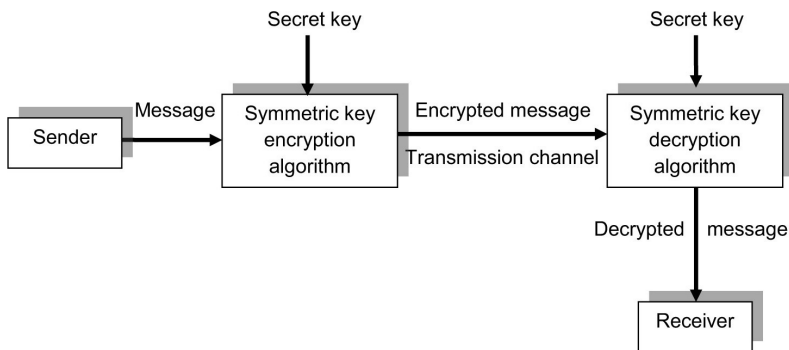


Figure 2-8. A symmetric key cryptosystem

Symmetric key encryption algorithms are fast compared to asymmetric key algorithms and are widely used to securely transmit large volumes of data. One popular symmetric key algorithm is the Advanced Encryption Standard (AES), which is specified in NIST Federal Information Processing Standards (FIPS) Publication 197¹¹. The standard specifies three symmetric key strengths of 128, 192, or 256 bits. AES has been adopted by private and public organizations inside and outside the United States and is widely used in smart cards, routers, and a variety of other applications.

Asymmetric Key Cryptography

As mentioned, asymmetric or public key cryptography uses a public and a private key. The public key can be accessed by anyone desiring to send an encrypted message to the holder of the corresponding private key. The important properties of a properly generated public-private key pair are summarized as follows:

- A message encrypted by one of the keys can be decrypted by the other key of the pair.
- The private key is kept confidential.
- The public key cannot be used to determine the private key.
- The public key cannot decrypt the message that it encrypted.

A typical asymmetric key cryptosystem is given in [Figure 2-9](#).

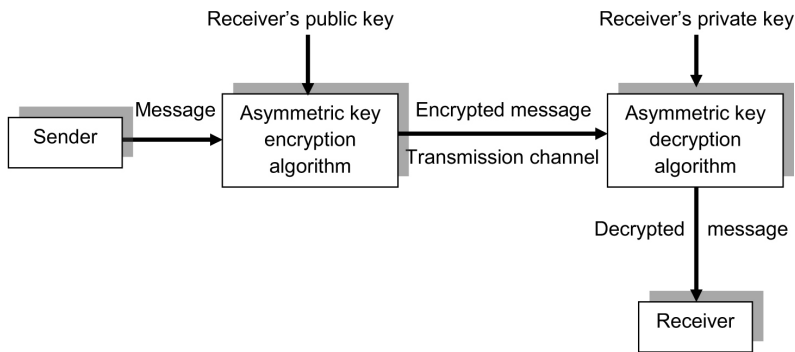


Figure 2-9. An asymmetric key cryptosystem

One of the most popular asymmetric key algorithms is the RSA algorithm, named after its developers, Rivest, Shamir, and Addleman¹². The strength of the RSA algorithm is based on the difficulty of finding the prime number factors of a large number, which would be required to generate the private key from the corresponding public key.

Asymmetric cryptographic key sizes have to be much larger than symmetric key sizes to obtain the same level of security. Table 2-4 lists the equivalent key strengths in bits of symmetric and asymmetric cryptographic systems to obtain the same level of protection through encryption.

An important application of asymmetric cryptography is in generating digital signatures.

Table 2-4. Symmetric vs. Asymmetric Key Sizes

Asymmetric key size
1024
2048
3072
7680
12360

[Source: NIST SP 800-57, *Recommendation for Key Management – Part 1: General (Revision 3)*, May 2011.]

Digital Signatures

The NIST Digital Signature Standard (DSS)¹³ defines a digital signature as “the result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data

integrity and signatory nonrepudiation.” A digital signature uses asymmetric key encryption to achieve nonrepudiation of a transmitted message and to authenticate the sender and receiver.

As part of the implementation of a digital signature, a variable-length message is fed into a type of encryption system, known as a hash function, which produces a shorter, fixed length output digital stream, a message digest. The message digest is uniquely bound to the input message, and any change in the input message will result in a change in the hash function output. This characteristic provides integrity checking and is also used to implement non-repudiation. The ideal characteristics of a hash function are:

- It is a one-way function because the original input file cannot be created from the message digest.
- Two files should not have the same message digest.
- The message digest should be calculated by using all of the original input file’s data.
- It should not be feasible to find another file with the same message digest, given a file and its corresponding message digest.

The digital signature of a message, M, is accomplished through the following steps:

- 1.Generate the message digest of M using a valid hash function.
- 2.Encrypt the message digest with the private key of the sender, and attach it to M.
- 3.Transmit M with the attached message digest.
- 4.Decrypt the message digest at the receiver’s end by using the sender’s public key. Because the public key of the sender is the only key that can open a file encrypted with the sender’s private key, the sender is authenticated.
- 5.Compute the message digest of M at the receiving end, using the same hash function as the sender.
- 6.Compare the message digest computed at the receiving end with the message digest transmitted by the sender together with message M. If the two message digests are identical, this verifies that the message was not modified after it left the sender.

Note that in this process, the message itself is not encrypted. [Figure 2-10](#)

summarizes the digital signature process.

An important issue that has to be addressed in using asymmetric cryptographic systems is the possibility that an individual, A, would falsely have the name of another person, B, attached to A's public key. Then, any messages sent to B could only be opened and read by A using A's private key. Thus, A would be reading all of B's messages. In order to thwart this kind of attack, an independent third party could be used to certify that a person's public key was actually the key associated with that person. This independent third party is known as a certificate authority and, if presented with the proper credentials, can warrant that an individual's public key is his or her valid public key and can generate a digital certificate to that effect. The certificate contains the subject's name, the subject's public key, the name of the certificate authority, and the period in which the certificate is valid. This certificate is then sent to a repository, which holds the certificates and certificate revocation lists (CRLs) that denote any revoked certificates.

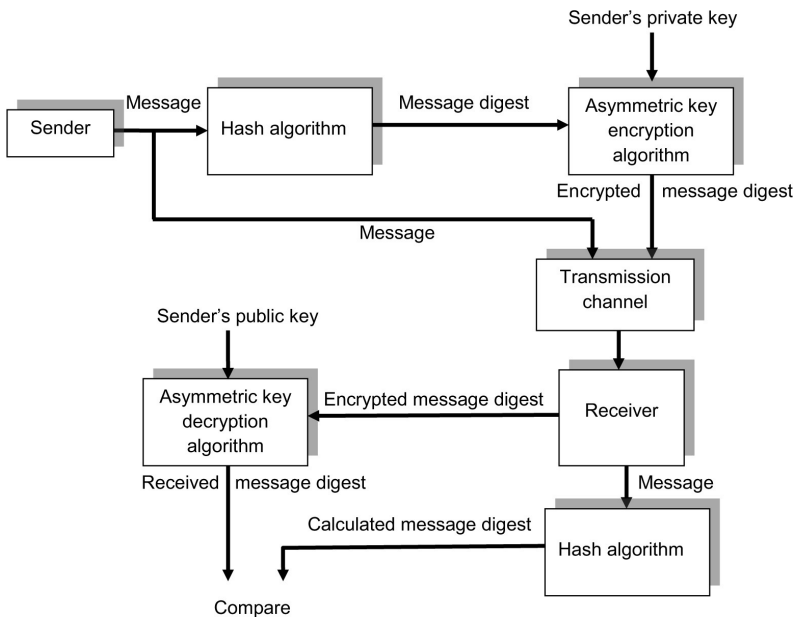


Figure 2-10. The digital signature process

Attacks Against Cryptosystems

The formal term for attacking cryptographic systems is cryptanalysis. In cryptanalysis, an attacker attempts to obtain the original, unencrypted message (plaintext) from the encrypted message (ciphertext). A number of approaches have been developed to perform cryptanalysis, from using mathematic

formulations to measuring electronic emissions from chips. The most common attacks are summarized as follows:

- Known plaintext attack – The attacker has access to samples of the unencrypted and encrypted versions of messages and uses this information to attempt to determine the key.
- Ciphertext only attack – The attacker has access to multiple samples of encrypted messages that have been encrypted with the same algorithm and attempts to find the key.
- Man-in-the-middle attack – The attacker intercepts messages being sent between two parties and attempts to decipher them and, possibly, to forward false messages to the parties.
- Replay attack – The attacker intercepts a message and sends it a later time.
- Chosen plaintext attack – The attacker has the ability to select plaintext messages, have them encrypted, and then analyze the results to determine the key.
- Chosen ciphertext attack – The attacker has the ability to select ciphertext messages for trial decryption while having access to the corresponding decrypted plaintext.
- Adaptive chosen ciphertext – The attacker conducts a chosen ciphertext attack but uses the results of one iteration to select the ciphertext to be used in the next iteration.
- Adaptive chosen plaintext – The attacker conducts a chosen plaintext attack but uses the results of one iteration to select the plaintext to be used in the next iteration.
- Differential cryptanalysis – The attacker analyzes ciphertext pairs generated by the encryption of plaintext pairs and attempts to use any differences in the ciphertext pairs to determine the key.
- Linear cryptanalysis – The attacker analyzes ciphertext pairs and their corresponding plaintext pairs to develop a linear approximation to portions of the key.
- Brute force – The attacker tries all possible combination of keys in hope of finding the correct key.

Encryption and digital signatures can be used effectively to transmit sensitive information securely over the Internet. One of the major means of accomplishing this type of transmission is the use of a virtual private network.

Virtual Private Network

NIST Special Publication 800-82¹⁴ defines a virtual private network (VPN) as:

A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.

ANSI/ISA-TR99.00.01-2007¹⁵ gives the following definition of a VPN:

A VPN is a private network that operates as an overlay on a public infrastructure. It contains three components, which are handled at the recipient end of the VPN:

- Authenticity and Authentication – Security measures designed to establish the validity of a transmission, message, originator, or a means of verifying an individual's authorization to receive specific categories of information.
- Integrity – In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.
- Confidentiality – Assurance that information is not disclosed to unauthorized persons, processes, or devices.

A secondary component of VPNs is authorization, which encompasses:

- The rights granted to a user to access, read, modify, insert, or delete certain data, or to execute certain programs
- Access privileges granted to a user, program, or process

In other words, the purpose of a VPN is to provide a user with the ability to use a public network, such as the Internet, to transmit and receive information that must be protected from compromise. A typical VPN is illustrated in [Figure 2-11](#).

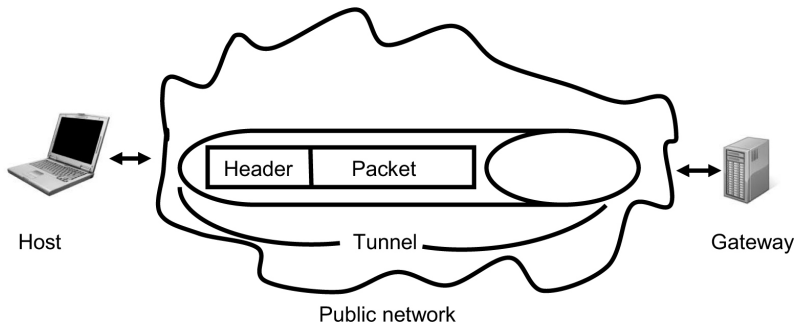


Figure 2-11. A typical virtual private network

There are three general types of VPNs:

- **Gateway-to-gateway** – Provides secure communications over a public network between two trusted networks, such as between two organizations.
- **Host-to-gateway** – Also known as a remote access VPN, provides secure communication between a host computer and an organization's network. An example of this type of VPN is a traveling salesman connecting his laptop to the organization's network from a remote location.
- **Host-to-host** – Enables secure communication between two computers over an untrusted network.

The characteristics of VPNs lend themselves to their use in industrial automation and control systems through their ability to establish secure communications between host systems and controllers over the Internet.

A VPN uses a tunnel through the public network to transmit the data to be protected. Establishing a tunnel, or tunneling, consists of encapsulating packets of a particular VPN protocol inside headers and transmitting the packets over another carrier protocol. The transmission takes place over a logical network connection established between the VPN client and server. The information being sent may be encrypted or not encrypted. For maximum security, the packets should be encrypted using an approved algorithm and a strong key. At the destination host, the reverse procedure takes place and the packets are unencapsulated and decrypted, if necessary. Two of the most popular VPN technologies are the Internet Security Protocol (IPsec) and Secure Sockets Layer (SSL).

IPsec

IPsec operates at the OSI network layer and provides the following two modes of encryption:

- Transport mode – Encrypts the data segment of the packet to be transmitted and does not encrypt the header.
- Tunnel mode – Adds an additional header to the packet and encrypts the entire packet, including the original header.

IPsec operates with two security protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). AH can provide authentication of the source and integrity of packets and data; however, it does not use encryption. ESP supports encryption along with providing authentication and integrity. Of the two protocols, ESP is more commonly used.

Secure Sockets Layer

The Secure Sockets Layer (SSL) protocol was developed in 1994 by Netscape to provide for secure Internet transactions. SSL encrypts the packet contents and authenticates the server to the client using digital signatures and digital certificates. The Internet Engineering Task Force (IETF)¹⁶ modified SSL 3.0 to produce the Transaction Layer Security (TLS) protocol, which has evolved to version 1.2¹⁷. SSL and TLS are popularly used to secure Internet HTTP communications and are known as HTTP secure (HTTPs). Information on applying TLS is given in NIST SP 800-52¹⁸.

Summary

[Chapter 2](#) has reviewed some of the basic tenets of information system security with the objective of developing a foundation for applying these methods, with appropriate adjustments, to harden and protect industrial automation and control systems. Many of the attack types reviewed in this chapter can be used against industrial automation and control systems in order to cause malfunctions, cause physical and economic damage, or even threaten lives. The countermeasures and techniques presented in [Chapter 2](#), properly applied, have the ability to improve the security posture of the systems controlling the nation's infrastructure and manufacturing facilities and thereby prevent or mitigate disruptive and damaging occurrences.

With the security concepts of this chapter in mind, [Chapter 3](#) will explore the similarities and differences between industrial automation and control system characteristics and requirements and those of IT systems.

Review Questions for Chapter 2

- 1.Information system security is defined as comprising which of the following three basic elements?
 - a.Confidentiality, integrity, and authorization
 - b.Confidentiality, integrity, and availability
 - c.Audit, integrity, and availability
 - d.Security, integrity, and availability
- 2.Protecting documents and messages from unauthorized disclosure refers to which of the following?
 - a.Confidentiality
 - b.Availability
 - c.Authorization
 - d.Integrity
- 3.An attack that overloads the resources of a computing system is an attack against which of the following?
 - a.Integrity
 - b.Availability
 - c.Confidentiality
 - d.Authentication
- 4.Which of the following items refers to the act of verifying a user's identity and confirming that a user is who he or she professes to be?
 - a.Authentication
 - b.Authorization
 - c.Registration
 - d.Accountability
- 5.Which of the following is a detective activity used to determine if violations of information system security have occurred?
 - a.Confirming
 - b.Authenticating
 - c.Auditing

d.Authorizing

6.Ensuring that the sender of a message or contract cannot later deny sending the message or contract is known as which of the following?

a.Nonrepudiation

b.Denial

c.Validation

d.Confirmation

7.A security control that minimizes the effect of an attack and the degree of resulting damage is known as which type of control?

a.Corrective

b.Preventive

c.Deterrent

d.Detective

8.The Information Assurance Technical Framework Forum (IATF) Document 3.1 ([Table 2-1](#)) defines which of the following attacks as an “attempt to circumvent or break protection features, introduce malicious code, or steal or modify information”?

a.Distribution

b.Close-in

c.Active

d.Passive

9.The act of establishing numerous layers of protection wherein a subsequent layer will provide protection if a previous layer is breached is known as which of the following?

a.Defense in depth

b.Complete mediation

c.Least privilege

d.Open design

10.Which of the following is noncompulsory?

a.Standards

- b.Guidelines
- c.Policies
- d.Procedures

11.A self-replicating or self-reproducing program that spreads by inserting copies of itself into other executable code or documents is known as which of the following?

- a.Worm
- b.Mobile code
- c.Back door
- d.Virus

12.An attack that focuses on the authentication protocol between a claiming party and a verifying party communicating with each other is known as which of the following?

- a.Meet-in-the-middle
- b.Man-in-the-middle
- c.Social engineering
- d.Brute force

13.NIST SP 800-41 defines which of the following as “devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures”?

- a.Firewalls
- b.Demilitarized zones
- c.Trap doors
- d.Browsers

14.What type of firewall filters packets based on firewall access control lists (ACLs), which specify the packets that can be sent to particular destination addresses, or on specific application port destinations?

- a.Stateful inspection
- b.Packet filtering
- c.Application proxy
- d.Screened-host

15. What type of firewall serves as an intermediary between networks and serves to mask the source of a message?
- a. Application
 - b. Packet filtering
 - c. Stateful inspection
 - d. Application proxy
16. What type of firewall defines a demilitarized zone (DMZ) or perimeter network, which is a third network that lies between the internal trusted network and the external untrusted network as an added layer of protection?
- a. Dual-homed host
 - b. Screened-subnet
 - c. Screened-host
 - d. Application
17. What type of cryptography uses public and private key pairs?
- a. Symmetric
 - b. Asymmetric
 - c. Secret key
 - d. Transposition
18. The Advanced Encryption Standard (AES) is an example of which of the following types of cryptography?
- a. Symmetric key
 - b. Asymmetric key
 - c. Public key
 - d. Dual key
19. The result of a variable length message being fed into a hash function is a shorter, fixed length output digital stream, known as which of the following?
- a. Ciphertext
 - b. Plaintext

c.Message digest

d.Cryptovvariable

20.A digital signature uses asymmetric key encryption to achieve which of the following?

a.Nonrepudiation

b.Nonrepudiation and authentication

c.Authorization

d.Confidentiality

21.A cryptographic attack in which the attacker uses multiple samples of encrypted messages that have been encrypted with the same algorithm to attempt to find the key is known as which of the following?

a.Chosen ciphertext

b.Ciphertext only

c.Adaptive chosen ciphertext

d.Known plaintext

22.A private network that operates as an overlay on a public infrastructure is known as which of the following?

a.Virtual private network

b.Dual band network

c.4G network

d.Demilitarized zone

23.IPsec provides which of the following two modes of operation?

a.Symmetric key mode and transport mode

b.Authentication mode and tunnel mode

c.Transport mode and tunnel mode

d.Transport mode and transparent mode

24.A VPN that provides secure communications over a public network between two trusted networks is known as which of the following?

a.Host-to-host

- b. Gateway-to-gateway
- c. Host-to-gateway
- d. Host-to-demilitarized zone

References

- 1 NIST Special Publication 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*, July 2006.
- 2 National Security Agency, *Information Assurance Technical Framework (IATF)*, Release 3.1, September 2002.
- 3 Saltzer, J.H. and Schroeder, M.D. *The Protection of Information in Computer Systems*, Fourth ACM Symposium on Operating Systems Principles, October 1974.
- 4 NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*, Final Public Draft, September 2008.
- 5 ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, October 2007.
- 6 NIST Special Publication 800-123, *Guide to General Server Security*, July 2008.
- 7 NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.
- 8 NIST Special Publication 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*, July 2006.
- 9 ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, October 2007.
- 10 NIST Special Publication 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.
- 11 NIST Federal Information Processing Standard Publication 197, *Advanced Encryption Standard (AES)*, November, 2001.
- 12 Rivest, R. L., Shamir, A., and Adleman, L. M. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, v. 21, n. 2, February 1978, pp. 120–126.
- 13 NIST Federal Information Processing Standard Publication 186-3, *Digital Signature Standard (DSS)*, June 2009.
- 14 NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*, Final Public Draft, September 2008.
- 15 ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, October 2007.
- 16 The Internet Engineering Task Force, www.ietf.org.

- ¹⁷ The Internet Engineering Task Force, Network Working Group, RFC 5246, *The Transport Layer Security (TLS) Protocol*, Version 1.2, August 2008.
- ¹⁸ NIST Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005.

Chapter 3

Industrial Automation and Control System Culture versus IT Paradigms

Some of the basic principles of information system security were presented in [Chapter 2](#) as a prelude to selectively and properly applying them to securing industrial automation and control systems. As a prerequisite to this adaptation, it is important to examine the differences in culture, requirements, and operational issues between automation and control systems and IT systems. Critical areas that have to be addressed include safety, real-time demands, maintenance, productivity, training, and personnel mindsets. These topics and related subject areas are discussed in this chapter to help the reader better understand how to apply security principles to automation and control systems without negatively impacting their primary mission and in full acknowledgement of their special requirements.

Differences in Culture, Philosophy, and Requirements

The major advances in securing computer systems and networks have come through the information system technology route, with origins in computer science and software engineering. The principal players are IT system administrators, systems analysts, database administrators, software engineers, network administrators, CIOs (chief information officers), and so on. On the other hand, a large number of the personnel populating the industrial automation and control system field come from engineering backgrounds, with training in such areas as electrical engineering, chemical engineering, mechanical engineering, systems engineering, and control engineering.

The motivation, requirements, and focus of each of the groups are, in many instances, largely divergent, with some overlapping common areas. For example, software quality and process improvement methods widely used in the IT environment are often foreign to control engineers and in fact may be viewed as cumbersome in implementing SCADA and process control algorithms. In addition, the performance of a process in a plant is critical, and inadequate performance in production areas can result in huge financial

losses, equipment damage, and personnel injuries. These severe consequences of operational errors are not usually a common occurrence in IT facilities. Similarly, safety is a critical concern in a production environment, and control system malfunctions can result in fires or explosions in some instances. Thus, in a production environment, safety and performance usually take precedence over information security, which is not the case in an information system.

Table 3-1. Comparison Between IT and Industrial Control and Automation Systems Issues

Application of the system is not at all. Delays caused by encryption software are a consideration.

Figure 3-1 summarizes the important issues listed in Table 3-1 and emphasizes some of the common areas between IT and automation and control systems.

The lesson to be learned from these comparisons is that traditional information system security knowledge and methods provide a solid basis for addressing industrial automation and control system security, albeit with deliberate, appropriate, and intelligent modifications required to address the unique characteristics of automation and control systems.

One important starting point in incorporating these modifications is education. In general, most universities and certification programs addressing computer and network security have been heavily focused on IT security. Automation and control systems, which are typically sitting on isolated networks and are relatively few in number compared to IT systems, have not been considered to be interesting targets. With the advent of the terrorism threat, this situation is no longer the case. In addition, SCADA and plant process control systems are now being connected to large networks and the Internet.

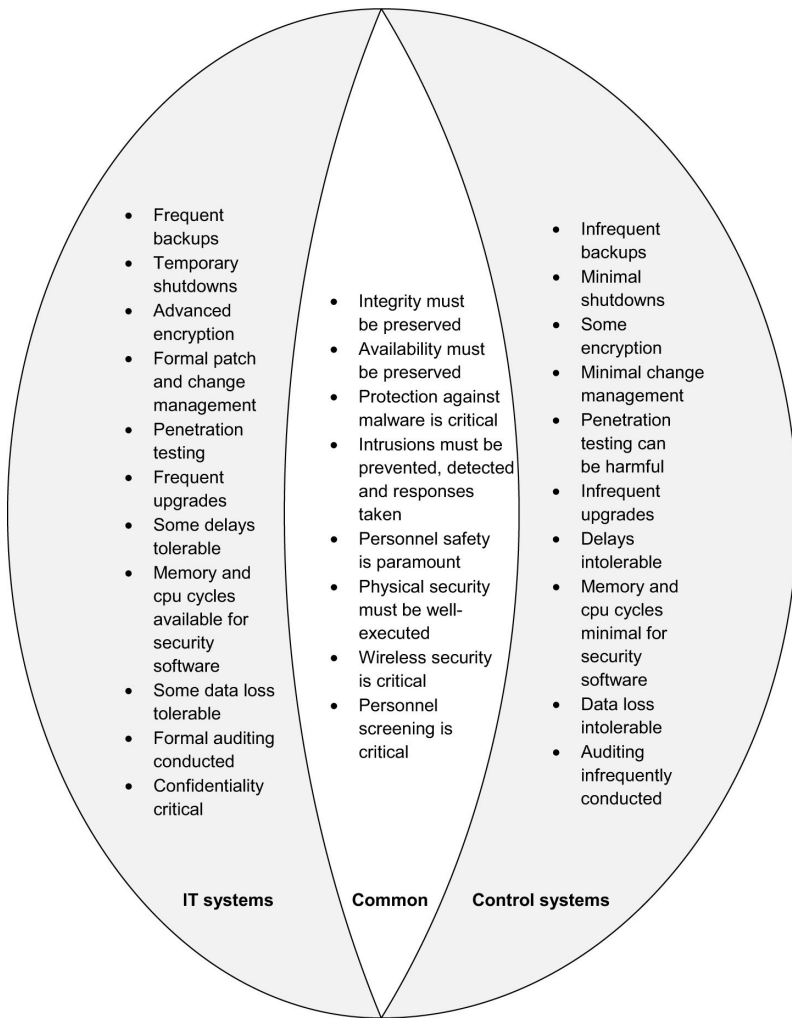


Figure 3-1. IT and automation and control system issue comparisons

The Certified Information System Security Professional (CISSP) and related certifications do not address the security of industrial automation and control systems. Organizations, such as ISA, have addressed this problem and are filling a critical need. NIST has generated special publications that directly address industrial automation and control systems. However, it is important that security training related to the control of production lines, industrial processes, electrical transmission and distribution, pipelines, chemical plants, and so on moves to the fore in universities, technical institutes, and certification organizations.

To understand how to adapt IT security methods to industrial automation and control system security, threats to the latter have to be identified and understood. One impediment to full disclosure of threats realized is the fact that a majority of affected facilities are privately owned, and these organizations are reluctant to publicize security breaches that could negatively affect their reputation and value.

Organizations also need incentives to invest in upgrading their automation and control infrastructure. Many existing installations have been in place for ten or twenty years, and investments in security have to compete with other compelling initiatives in an organization.

Considerations in Adapting IT Security Methods to Industrial Automation and Control Systems

In order to secure industrial automation and control systems (IACS), there are specific issues that have to be addressed that take into account the differences between IT systems and IACS. These issues include the following:

- Accountability, authorization, and computer forensics have not matured and have not been implemented widely in IACS as compared to IT systems.
- Ethernet to serial line paths provide a means of injecting malicious commands into a control network.
- Excessive checking, encryption, monitoring, and so on can interfere with the deterministic nature of process control systems.
- In many IACS environments, control engineers have multiple responsibilities that, in many instances, violate the security principle of separation of duties.
- Installing patches and upgrades in process control systems can lead to serious and sometimes dangerous situations in production facilities.
- Life cycle design disciplines common in the IT field are not widely used in industrial automation and control systems.
- Maintenance hooks and trap doors installed in automation and control systems for remote maintenance can be easy entry points to modify critical software and firmware with negative consequences.
- Many IACS vendors combine safety mechanisms with security mechanisms, leading to single points of failure and less

resiliency than separating these two functions logically and physically.

- Many manufacturing facilities and SCADA installations house legacy systems with outdated technology, minimal memory and computing power, and little thought to security.
- Port scanning of automation and control systems can result in blockages and lack of system availability.
- Remote access into automation and control systems via older modems or newer wireless devices poses a serious threat to security.
- There is a trend to apply protocols used for IT systems to industrial control and automation systems because of their wide availability, their lower cost, and the existence of trained personnel. However, these protocols, in most instances, were not designed for deterministic process control systems and also are vulnerable to many existing attacks.
- There is heavy reliance on suppliers, who provide modified software and hardware for IACS, resulting in nonstandard implementations that are difficult to maintain without support from these suppliers.
- Weak authentication mechanisms in many SCADA systems and networked plant control systems leave them vulnerable to attack.

A variety of additional items must be considered when discussing comparisons between IT and industrial automation and control systems. The concepts related to risk management and the means to protect industrial automation and control systems will be discussed in detail in [Chapters 5 and 6](#), respectively. However, it is important to now examine some related critical subject areas to provide a basis for developing more specific security solutions.

Threats

Threats to IT and industrial automation and control systems come from different sources, with different motivations. It is important to understand these threat sources and their characteristics in order to counter any malicious activities on their part. NIST SP 800-30¹ summarizes the various types of threat sources and some of their driving factors as shown in [Table 3-2](#). [Table 3-3](#), also from NIST SP 800-30, provides a listing of some general threat sources, including environmental ones, which can also cause disruptions to industrial automation and control systems.

The categories of terrorists, industrial espionage, and insiders are of particular

interest in connection with industrial automation and control systems. Traditionally, insider threats have been considered one of the most dangerous because they give insiders the ability to bypass protective measures. However, external threats are increasing and are also of grave concern, particularly relating to our nation’s critical infrastructure and resource processing plants. In addition, threats to automation systems can materialize from environmental and structural sources as illustrated in the next section.

Sensitivity of Industrial Automation and Control Systems to Upgrades and Modifications

One area that is not usually considered when discussing the relative sensitivities of IT systems and industrial automation and control systems are the effects of equipment upgrades and modifications. A particularly relevant example concerns the consequences of converting analog controls to digital controls. Digital systems transfer information via pulses, which inherently generate high frequency electromagnetic radiation that can interfere with control system operations. An article in the journal *Interference Technology*² describes the electromagnetic radiation emission environment in a nuclear plant that was being changed from analog to digital controls. The authors obtained measurement data in the range of 100 Hz to 6 GHz in instances before and after the conversion.

Table 3-2. Threats and Motivations for Attackers

Threat	Motivation
•Hacker	•Curiosity
•Social engineering	•Financial gain
•System intrusion, break-ins	•Revenge
•Unauthorized system access	•System tampering
•Computer crime (e.g., cyber stalking)	•Disruption of operations
•Illegal information disclosure, impersonation, interception	•Espionage
•Identity theft	•Financial gain
•Data tampering	•Revenge
•System intrusion	•System tampering
•Hostile terrorism	•Disruption of operations
•Information warfare	•Disruption of operations
•System attack (e.g., distributed denial of service)	•Disruption of operations
•System penetration	•Disruption of operations
•System tampering	•Disruption of operations
•Disruption of operations (e.g., companies, foreign governments, other government interests)	•Disruption of operations
•Information warfare	•Disruption of operations
•Intrusion on personal privacy	•Disruption of operations
•Social engineering	•Disruption of operations
•System penetration	•Disruption of operations
•Unauthorized system access (access to classified, proprietary, and/or technology-related information)	•Disruption of operations
•Disruption of operations (e.g., disgruntled, malicious, negligent, dishonest, or terminated employees)	•Disruption of operations
•Breach of proprietary information	•Disruption of operations
•Data tampering	•Disruption of operations

Revenge and theft

Unintentional entry and omissions (e.g., data entry error, programming error)

- Input of falsified, computed data
- Interception
- Malicious code (e.g., virus, logic bomb, Trojan horse)
- Sale of personal information
- System bugs
- System intrusion
- System sabotage
- Unauthorized system access

[Source: NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2011.]

The testing followed guidelines in U.S. Nuclear Regulatory Commission Regulatory Guide, NUREG 1.1803 and Electric Power Research Institute (EPRI) document TR-102023-20044. In the tests, antennas were installed next to three cabinets housing control electronics, and radiation emission measurements were taken from the analog and digital control installations. Some of the results obtained are summarized in Table 3-4, showing frequencies at which peak amplitudes occur at antennas 1 and 2.

Table 3-3. Listing of General Threat Sources

Type	Description
Adversary	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).
Trusted Insider	
Privileged Insider	
Group	
Ad hoc	
Established	
Organization	
Nation-State	
Responsible	Actions taken by individuals in the course of executing their everyday responsibilities.
Privileged User/Administrator	
Equipment	Hardware, equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.
Storage	
Processing	
Communications	
Display	
Sensor	
Controller	
Environmental Controls	
Temperature/Humidity Controls	
Power Supply	
Software	
Operating System	

- Networking
 - General-Purpose Application
 - Mission-Specific Application
- Range of Events** and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
- Notes:** Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
- Windstorm/Tornado
 - Earthquake
 - Bombing
 - Overrun
 - Unusual Natural Event (e.g., sunspots)
 - Infrastructure Failure/Outage
 - Telecommunications
 - Electrical Power
- [Source: NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2011.]

Table 3-4. Radiation Emission Measurements

Antenna	Analog measurement		Digital measurement	
	Frequency	Significant peak amplitudes (dBμV/m)	Frequency	Significant peak amplitudes (dBμV/m)
1	1.34 MHz	99.2	468 MHz	71.6
1	928 MHz	76.6	826 MHz	94.5
1			928 MHz	113.5
1			1.35 GHz	49.9
1			1.88 GHz	50.5
1			1.92 GHz	53.4
1			2.41 GHz	76.3
1			2.46 GHz	54.4
1			5.82 GHz	60.6
2	1.04 MHz	99.3	2MHz	84
2	4.55 MHz	88.5	10MHz	80
2			1GHz	109
2			1.17 GHz	48.8
2			1.92 GHz	48.9
2			2.42	57.7
2			5.82 GHz	50.9
[Source: Keebler, P. and Berger, S. "Going from Analog to Digital," <i>Interference Technology, 2011 EMC Directory and Design Guide</i> , 2011.]				

This data is plotted in [Figures 3-2](#) and [3-3](#) for antennas 1 and 2, respectively. Note that the digital electronics generate more peak radiation generally and more at high frequencies compared to the analog equipment. These peak emissions have the potential to interfere with control system signals and cause malfunctions if proper shielding and isolation are not applied.

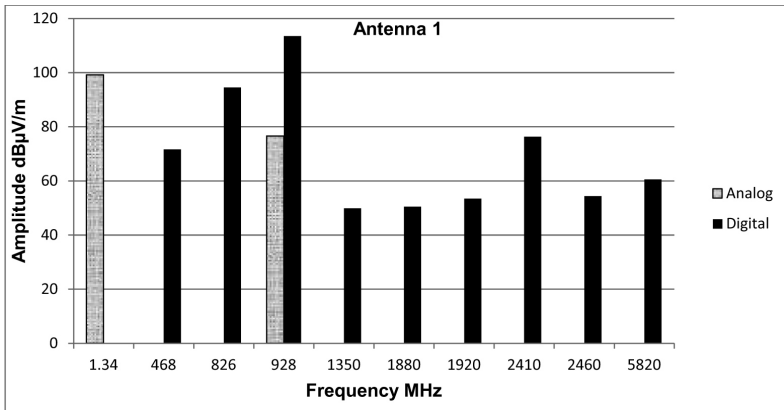


Figure 3-2. Analog and digital radiation emissions received at antenna 1

The sample electromagnetic emanations collected illustrate the necessity to ensure electromagnetic compliance (EMC) when equipment upgrades are made to plant control systems. These actions will serve to protect against interruptions of control systems' operation because of electromagnetic emissions from digital systems.

IT and Industrial Automation and Control Systems Comparisons from a Standards Perspective

Valuable insight into the contrasts and similarities between IT systems security focus areas and those of industrial automation and control systems can be obtained from an example using standards that represent each of the areas. In this example, ISO/IEC 27002, *Code of Practice for Information Security Management*⁵ will be used to represent IT systems security areas of emphasis while ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*⁶, will be used to illustrate the major concerns of automation and control system security.

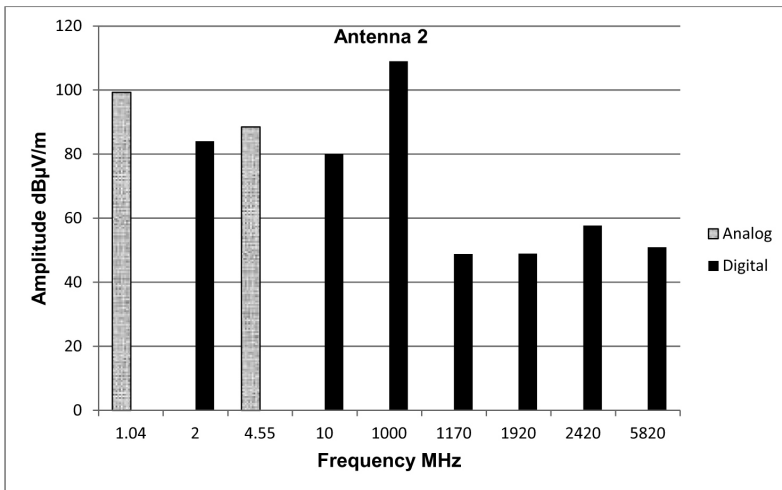


Figure 3-3. Analog and digital radiation emissions received at antenna 2

In each document, there are common areas addressed by both standards and other areas addressed by one and not the other. [Figure 3-4](#) summarizes the main characteristics of each standard and identifies common areas addressed by both as well as topics that are addressed mainly by one document and not the other.

[Figure 3-4](#) shows that topics, such as change management, email security, access control policies, digital signatures, compliance, and business continuity planning are among the areas considered critical for IT systems that are not emphasized in automation and control system standards. Conversely, for automation and control systems, the significant domains not covered include security architecture analysis, quantitative and qualitative analysis, information security management, and information security testing. Areas of common emphasis include information security policy, risk assessment, training, media physical security, remote access, event logging, and protection against malware.

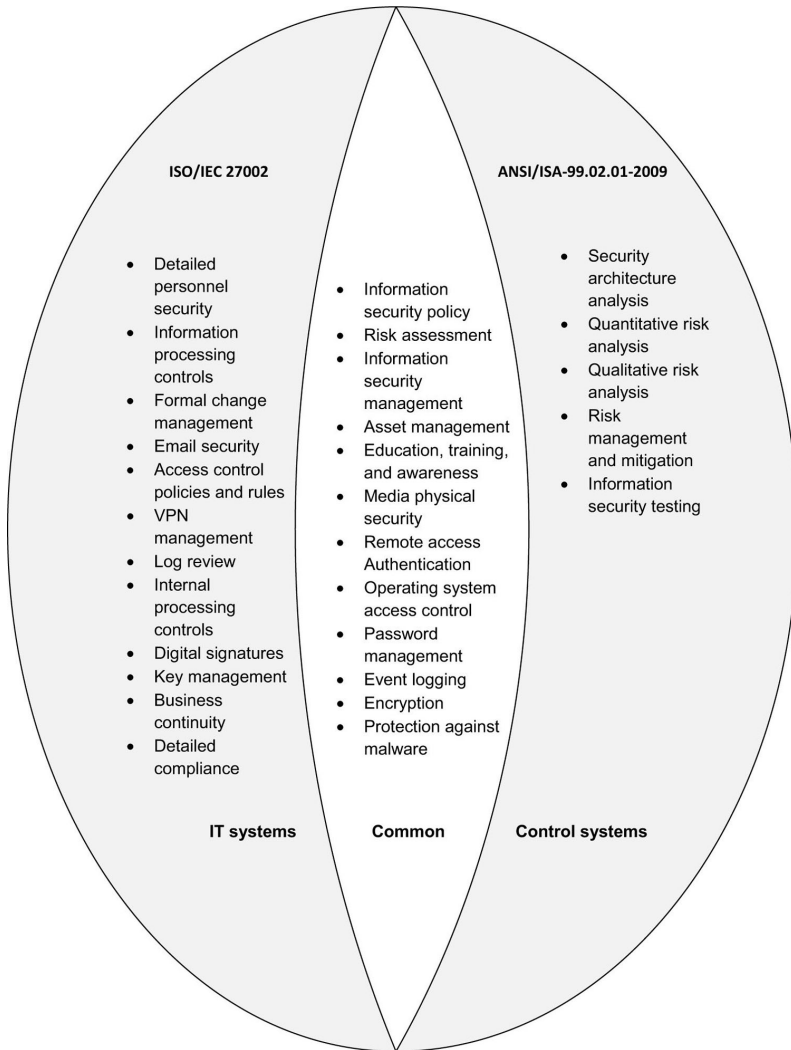


Figure 3-4. Standards comparison example of IT vs. IACS important security areas

Summary

Understanding the requirements of industrial automation and control systems security and how they relate to IT systems supports a mapping of these requirements onto the emerging technologies being employed in the control of production processes as well as the critical infrastructure (represented primarily by the electrical generation and distribution grid). The advances in capability and sophistication of industrial automation and control systems require a tailored approach to security. Some of the factors pushing the

industrial automation and control systems security envelope include:

- The Smart Grid
- Advanced cryptography and key management applications
- Advanced PLCs and PACs
- Advanced protective relaying
- Advanced wireless networks
- Alarm processing
- Availability of real-time energy information
- Multisphere security among IT, transportation, and power systems
- Redundancy in networks, equipment, and sensors
- Fiber communication
- Use of GPS tracking

Chapter 4 will investigate the technical evolution taking place in elements of the critical infrastructure and in key production facilities to identify the important risk factors and areas of maximum potential impact in the event of an attack.

Review Questions for Chapter 3

1. Which of the following statements is generally TRUE regarding an industrial automation and control system?
 - a. Installation of software patches can be performed routinely and frequently.
 - b. Encryption of data can sometimes lead to problematic delays.
 - c. Penetration testing can be conducted routinely and frequently.
 - d. Confidentiality is a key concern in automation systems as opposed to integrity and availability.
2. In both IT and automation and control systems, which of the following is the primary concern in the event of an emergency or malicious event?
 - a. Equipment safety

- b.Preservation of documentation
- c.Personnel safety
- d.Facility protection

3.Which of the following statements is FALSE?

- a.Flash drives and other portable memory devices can be sources of malware injections into control systems.
- b.Maintenance hooks and trap doors installed in automation and control systems for remote maintenance can be easy entry points to modify critical software and firmware with negative consequences.
- c.In many control system environments, control engineers, in general, do not have multiple responsibilities, such that the security principle of separation of duties is not normally violated.
- d.Many facilities house legacy systems with outdated technology, minimal memory and computing power, and little thought to security.

4.Which of the following actions is the most likely to result in blockages and lack of system availability in automation and control systems?

- a.Remote access
- b.Life cycle design
- c.Accountability
- d.Port scanning

5.Which threat source is motivated by revenge, ego, and dissatisfaction?

- a.Insider
- b.Espionage
- c.Criminal
- d.Hacker

6.What is a source of a possible disruption of control system functions that is not normally considered?

- a.Changes from digital to analog systems
- b.Upgrades from analog to digital systems

c.Malware

d.Attacks

7.In general, what distinguishes analog control equipment from digital control equipment?

a.Analog controls generate more high-frequency peak voltages than digital controls.

b.Digital controls generate more high-frequency peak voltages than analog controls.

c.Analog controls generate essentially the same number of high-frequency peak voltages as digital controls.

d.Digital controls generate essentially the same number of high-frequency peak voltages as analog controls.

8.Which of the following is more likely to be performed in an IT environment than in an automation and control system environment?

a.Security architecture analysis

b.Information security testing

c.Quantitative risk analysis

d.Change management

9.Which of the following is more likely to be a common area of security practice that is equally performed in both IT and automation and control systems?

a.Information security management

b.Information processing controls

c.Email security

d.Digital signatures

10.Which of the following threat sources is motivated by economic exploitation and competitive advantage, and uses social engineering?

a.Insider

b.Terrorist

c.Industrial espionage

d.Computer criminal

11. What is a detective control that is more frequently applied in IT systems than in control and automation systems?
- a. Firewall
 - b. Separation of duties
 - c. Biometrics
 - d. Auditing
12. Which of the following is NOT a usual reason for an organization's reluctance to disclose successful attacks against it?
- a. Hope the attack will harm competitors
 - b. Embarrassment
 - c. Effect on reputation
 - d. Possible loss of customers
13. Which of the following can lead to a single point of failure in an industrial automation and control system?
- a. Separation of duties
 - b. Disk redundancy
 - c. Combination of safety and security mechanisms
 - d. Use of authentication with identification
14. What is a typical characteristic of industrial automation and control systems?
- a. Have excess computing cycles
 - b. Have limited extra computing cycles
 - c. Have excess memory
 - d. Computational speed is not an issue
15. What is a typical characteristic of an automation and control system supplier?
- a. Usually ensures maintenance hooks are never left enabled without the customer's approval
 - b. Usually ensures default passwords are never duplicated from one customer to another

- c. Usually provides unmodified off-the-shelf hardware and software
- d. Usually provides modified hardware and software

References

- 1 NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2011.
- 2 Keebler, P. and Berger, S. “Going from Analog to Digital,” *Interference Technology, 2011 EMC Directory and Design Guide*, 2011.
- 3 U.S. Nuclear Regulatory Commission (NRC) Regulatory Guide, NUREG 1.180, *Guidelines for Evaluating Electronic and Radio Frequency Interference in Safety-Related Instrumentation and Control Systems*, Rev. 1, October 2003.
- 4 EPRI TR-102323-2004, Rev. 3, *Guidelines for Electromagnetic Interference Testing in Power Plants*, 2004.
- 5 ISO/IEC Standard 27002-2005, *Information Technology – Security Techniques - Code of Practices for Information Security Management*, 2005.
- 6 ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, 2009.

Chapter 4

The Continuing Technological Evolution Affecting the Industrial Automation and Control Systems

Chapter 3 presented the important differences between IT systems and industrial automation and control systems, along with some areas that are common to both of them. However, it is important to recognize that these differences are based on elements in both technologies that are constantly evolving. Thus, in order to truly understand and safeguard automation and control systems, these technology drivers and their potential effects on the components of the critical infrastructure have to be identified and examined. Chapter 4 investigates these areas and focuses on technological issues that relate directly to the security posture of the critical infrastructure, using the Smart Grid as an example.

Important Technological Trends

At any point in time, as technological advances occur and the technologies are adopted, related issues often appear. In this chapter, some of the major technological trends and associated concerns that directly and indirectly affect (or will affect) the industrial automation and control system landscape are examined. Then, the Smart Grid initiative will be explored relative to these technological developments as an example in the automation and control systems field.

Some of the emerging technological trends and associated concerns that will have a significant impact on both business and industry are home area networks, energy storage, analytics, cloud computing, privacy, social networks, mobile technology, and interoperability.

Home Area Networks

An increasing number of homes have a home area network (HAN) to some extent. The most common implementation is connecting devices, such as PCs, printers, laptops, tablet devices, Internet telephones, smart phones, and game computers. Additional items that are being connected and that will be more commonly connected in the future are digital video recorders, TV sets, and

network attached storage (NAS) devices.

Relative to the Smart Grid, home area networks are being viewed as important network elements to connect to smart meters. It is anticipated that the home area network will host smart thermostat controls, user information displays, and interfaces to remotely control such items as appliances, lighting, and security systems. With this capability, a smart meter could communicate with appliances over the home area network to reduce energy consumption during periods of peak demand while also supplying information to customers, service providers, suppliers, and utilities. Customers could use this information to alter usage patterns and reduce energy costs.

Energy Storage

Energy storage device technology is advancing because of the needs of hybrid and electric vehicles. In addition, finding a means to capture and store intermittent, renewable energy is driving such technologies as “super” batteries and ultracapacitors as well as other devices. The advent of the Smart Grid has put a new emphasis on efficient energy storage methods that can be applied at various points in the Grid to supplement conventional electricity generation methods.

Analytics

Analytics is the application of data mining and analysis to large amounts of data for the purposes of discovering knowledge and making intelligent predictions and decisions. Because large volumes of data are being generated and captured in very short amounts of time in automation and control systems, being able to analyze this data and make sound decisions based on this analysis is becoming increasingly important and necessary. A typical example is using analytic tools to visualize data within databases, networks, and applications and to make critical decisions in real time. A related issue is the ability to meaningfully display acquired information and share it among colleagues to support collaboration and innovative decision making.

Traditionally, analytics has been applied in electrical power systems for condition monitoring of high voltage electrical equipment. However, analytics holds promise for more sophisticated support of industrial automation and control systems to support rapid decision making and to provide an instinctively understandable visualization of critical information. Specifically, data collected on the Smart Grid through wireless, optical fiber, and other communication means can provide data on the health of Grid components, such as transformers, as well as voltage monitoring and energy consumption information. This data can be used to identify areas of potential failure and to initiate corrective action before actual outages occur.

Analytics can also be applied to secure industrial automation and control systems in the form of cyber analytics. In cyber analytics, data from a variety

of sources can be analyzed in real time or near real time to perform predictive modeling and thereby support physical, logical, and administrative security.

Cloud Computing

The cloud computing paradigm is being embraced by many organizations, and this will affect how data is collected, stored, and processed in these organizations, including in automation and control systems. NIST¹ defines cloud computing as:

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

The NIST document defines the essential characteristics of cloud computing as:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without human interaction with each service's provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers, using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the consumer generally has no control over or knowledge about the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and

rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

The three NIST cloud service models are:

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

NIST defines the cloud deployment models as:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premises or off premises.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off premises.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an

organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Cloud computing emphasizes service and can result in lower costs, agility, and the ease of integration of business and industrial processes. It can also increase availability through the distribution of capabilities to areas both inside and outside of the organization. Availability can also be enhanced by the cloud's ability to automatically manage and transport virtual applications dynamically. This approach supports automatic failover, provisioning to adapt to load demands, enforcement of security policies, and monitoring of security violations.

The cloud can also provide exceptional resources in the implementation of analytics solutions.

Privacy

Privacy is becoming more and more important in the conduct of business and computer-related activities. Special precautions have to be taken to protect personally identifiable information (PII) in all types of environments to avoid violation of regulatory and compliance requirements, such as HIPAA. PII is information that can be used to identify an individual and discover sensitive information about that individual. It is imperative that the management of an organization ensures that proper and adequate controls are in place to protect this sensitive information. These controls must include robust identification and authentication mechanisms to protect both individuals and physical equipment. Disclosure of PII such as a user's password, social security number, address, and health situation can be used to compromise the person and eventually gain access to critical organizational information and equipment. Threats to computer systems continually evolve and are becoming more sophisticated. Intentional or unintentional employee actions can bypass protection mechanisms and cause serious physical and financial damage and loss or compromise of sensitive information.

An organization should have privacy policies in place that are a statement of management intent and commitment to protect PII. A privacy policy usually addresses what information is collected, email rules, what information is shared with partners, how information is protected, disclosure rules, and authentication mechanisms.

Most privacy policies embody the following five basic principles:

- Access – Individuals should be able to review and correct their PII.
- Choice – Individuals should have the choice to opt out or opt in on permitting the disclosure of their PII to other entities.
- Enforcement – Privacy rules should be enforced.
- Notice – Individuals should be kept informed of the disclosure and use of PII.
- Security – Unauthorized disclosure of PII should not occur.

The European Union (EU) has codified privacy principles that apply to their citizens. These principles are:

- Data should be collected in accordance with the law.
- Data should be used only for the purposes for which it was collected, and it should be used only for a reasonable period of time.
- Individuals are entitled to receive a report on the information that is held about them.
- Individuals have the right to correct errors contained in their personal data.
- Information collected about an individual cannot be disclosed to other organizations or individuals unless authorized by law or by consent of the individual.
- Records kept on an individual should be accurate and up to date.
- Transmission of personal information to locations where equivalent personal data protection cannot be assured is prohibited.

Because in the Smart Grid paradigm personal data will be collected, transmitted, and stored, privacy protection should be inherent in the Grid. The principles expounded in the previous paragraphs can serve as guidance in privacy implementations for the Smart Grid.

As discussed earlier in this chapter, cyber analytics can be useful in determining patterns and threat vectors from large and diverse sources of data to predict possible future attacks or compromises of PII.

Social Networks

Social networks are becoming widely used by individuals in all walks of life.

According to Facebook statistics², there are more than 500 million active users who spend over 700 billion minutes per month on Facebook. Social sites, such as Facebook, which many consider hobbies, can be sources of vital information and serve as platforms for collaboration, innovation, and rapid transactions. Incorporating such platforms and media into a corporate environment can provide benefits, such as providing business intelligence, conducting training, and enhancing communications among colleagues, customers, and partners. On the other hand, social networks can be points of vulnerability for attackers and serve as avenues for the compromise of sensitive information. Participation in social networks at all levels of an organization can impact the security and privacy of the organization by providing information that can lead to the disclosure of proprietary data.

Mobile Technology

Interactivity is becoming the norm in dealing with digital devices and systems. Users can communicate with systems through social media, touchscreens, and mobile devices. Accessing data and controlling automation and control systems easily through iPad-like interfaces from a variety of physical locations offer both opportunities and concerns. The proliferation of 4G WiMAX will make remote communications from mobile devices more common and allow messaging and controls to be available to a variety of personnel and applications. Transactions on these networks will have to be managed, and policies redesigned, to accommodate such communications.

Interoperability

Interoperability is the ability of an entity to exchange data with another entity. In the computer realm, this data exchange can consist of software applications communicating with each other through common protocols and file formats. With the advent of technologies such as cloud computing and mobile platforms, it is important not to tie applications to specific types of platforms and not to discourage moving applications among different computers, storage, and networks.

Historically, industrial automation and control systems were developed on hardware and software modified by vendors for targeted applications and could not be ported to other platforms.

In implementing advanced industrial automation and control systems for programs, such as the Smart Grid, it is critical that hardware and software are interoperable and are verified for interoperability through some of the following means:

- Use independent testing groups to evaluate interoperability of software and hardware products from different sources
- Statistically test samplings of combinations of applications for

interoperability and project the probability of the other similar combinations being interoperable

- Test all software items against a standard reference to determine interoperability
- Test hardware items against applicable standards to ensure interoperability

The security of interoperable software components poses a different set of issues. The question to be answered is how to determine the security posture of application software comprised of software components whose security has been evaluated. It is not always the case that the features and characteristics of the resultant composite model reflect the security characteristics of the component software elements. These issues are explored in detail in a paper by Oladimeji and Chung from the University of Texas³. In the paper, the authors demonstrate that using secure software components to build a large system does not always guarantee the security of the large system. They also present an approach that can be used to ensure that the security requirements of the composite system are fulfilled when using secure components or to show that some components might not satisfy the security specifications of the composite system.

The Smart Grid and Technological Trends

It is important to identify the effects of technological developments on industrial automation and control systems. Technology advances have been incorporated into the elements of the critical infrastructure and, in doing so, have increased performance and efficiency. Networks that were once isolated are now interconnected and, in many instances, manage data from a variety of organizations. A natural progression of this technological evolution is to use advanced automation and networking methods to optimize system operations. However, the improvements in performance obtained by these enhancements have to be considered in light of the impact of the new technologies on safety, security, cost, and long-term consequences. To provide an illustration of these issues, the Smart Grid technologies will be overlaid with the technological trends described in the first part of this chapter. The following discussion is not meant to be an exhaustive exploration of the Smart Grid, but is presented to provide enough detailed information to serve as a basis for exploring the consequences of technological evolution and applications on an advanced automation and control system.

In the NIST document *Framework and Roadmap for Smart Grid Interoperability Standards*⁴, the Smart Grid is characterized as “adding and integrating many varieties of digital computing and communication technologies and services with the power-delivery infrastructure. Bidirectional flows of energy and two-way communication and control capabilities will enable an array of new

functionalities and applications that go well beyond ‘smart’ meters for homes and businesses.” The NIST document also cites the following distinguishing characteristics of the Smart Grid as:

- Increased use of digital information and controls technology to improve the reliability, security, and efficiency of the electric grid
- Dynamic optimization of grid operations and resources, with full cybersecurity
- Deployment and integration of distributed resources and generation, including renewable resources
- Development and incorporation of demand response, demand-side resources, and energy efficiency resources
- Deployment of “smart” technologies for metering, communications concerning grid operations and status, and distribution automation
- Integration of “smart” appliances and consumer devices
- Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles and thermal-storage air conditioning. An example of peak shaving would be a hybrid electric vehicle sending power back to the grid when demand is high.
- Provision to consumers of timely information and control options
- Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid
- Identification and lowering of unreasonable or unnecessary barriers to the adoption of Smart Grid technologies, practices, and services

In summary, the idea of the Smart Grid is to automate the electric power system by providing the ability to monitor and optimize operations across the grid from bulk generation to the consumer through two-way transmission of electricity and information.

Some of the benefits of the Smart Grid are put forth as:

- Built-in cybersecurity
- Higher grid resiliency
- Higher power quality

- Improved energy delivery efficiency
- Improved generation efficiency
- Reduced emissions and pollutants
- Reduced operating costs

With the increased interconnectivity and linking of Smart Grid networks, there are increased risks. These risks are summarized as follows from the NIST Guidelines for Smart Grid Cybersecurity⁵:

- Increasing the complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors.
- Interconnected networks can introduce common vulnerabilities.
- Increasing vulnerabilities to communication disruptions and the introduction of malicious software/firmware or compromised hardware could result in denial of service (DoS) or other malicious attacks.
- Increased number of entry points and paths are available for potential adversaries to exploit.
- Interconnected systems can increase the amount of private information exposed and increase the risk when data is aggregated.
- Expansion of the amount of data that will be collected can lead to the potential for compromise of data confidentiality, including the breach of customer privacy.

Relative to the C-I-A triad of confidentiality, integrity, and availability, availability will be the most important of the three principles in the Smart Grid environment. Data integrity is also important while confidentiality ranks third in the list, in general. For confidentiality, encryption keys will be used in the Smart Grid, and management of the large numbers of keys involved will be an important task.

NIST has developed a framework for the Smart Grid as shown in [Figure 4-1](#).

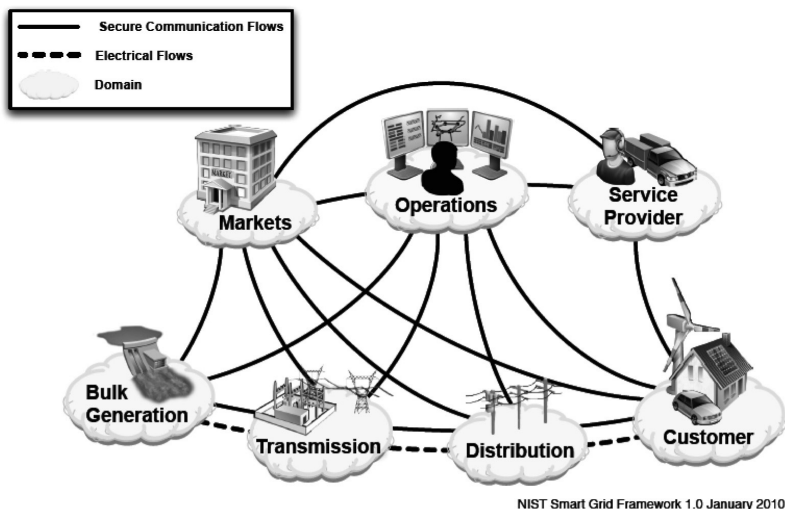


Figure 4-1. Smart Grid interactions and electrical flow

In [Figure 4-1](#), customers have the historical role of consuming electricity. However, in the Smart Grid architecture of [Figure 4-1](#), the customer can also be a source of electricity that can be generated and stored at the customer's site. Operations are responsible for managing the movement of electricity in the Smart Grid, and markets refer to the markets for selling and buying electricity. Bulk generation produces and stores electricity and uses transmission systems to move the electricity over large distances. Then the electricity is taken from the Transmission system and provided to the customer through the distribution system. A summary of the roles of these domains is given in the following sections.

Bulk Generation

The bulk generation domain principally connects to and communicates with the transmission and operations domains, but it also communicates with some of the other domains as shown in [Figure 4-1](#). Bulk generation provides energy generated from sources such as coal, gas, water from dams, nuclear reactions, geothermal, the sun, and wind. In the Smart Grid environment, bulk generation must also be able to store energy from sources that are not continuously available.

SCADA systems are employed in the bulk generation domain to control and measure its subsystems and exchange data with the operations domain.

The Transmission Domain

The transmission domain delivers electrical power from the bulk generation

domain to the distribution domain and balances the required electrical load between these two entities. It also provides energy storage capabilities. There is close coordination between the transmission domain and the operations domain. The transmission domain incorporates transformer substations that step up the voltage for transmission and then step-down the voltage for the distribution domain.

Additional energy supplies required by the transmission domain are obtained through the marketing domain. Transmission networks are usually run by a Regional Transmission Operator or Independent System Operator (RTO/ISO).

The Distribution Domain

The distribution domain serves as the intermediary between the transmission and customer domains and is normally connected in a radial configuration with customers and their metering systems. However, with the capabilities of the Smart Grid, the interaction of the distribution domain with the customer can also be a mesh or loop and through wired or wireless networks. This domain also will connect to energy storage facilities.

The Operations Domain

The operations domain provides reliable and high-quality power delivery on the Grid and interacts with all other domains of the Grid. Historically, operations have been the responsibility of a regulated utility, but they can also be the function of a service provider. This domain provides for locating faults, monitoring equipment, such as breakers and switches, evaluating security, keeping inventory, scheduling maintenance, monitoring intelligent field devices, gathering business intelligence, and optimizing Grid performance.

The Service Provider Domain

The service provider domain communicates with the operations domain, if they are separate entities, to provide the basis for controlling critical elements of the Grid. It also interacts with the markets and customer domains to provide account management and billing. Additional functions performed by the service provider domain include:

- Handling customer problems
- Maintenance and installation of customer premises devices
- Managing business accounts
- Providing building and home energy management

The Markets Domain

The markets domain buys and sells energy services and communicates with

the other domains to balance supply and demand. Additional functions provided by this domain include:

- Establishing pricing mechanisms
- Managing regulation issues
- Providing roaming billing information
- Providing secure communication with other domains
- Supporting interoperability across suppliers of market data

The Customer Domain

The customer domain is where the electricity is used and where customers can manage their electricity usage and electricity generation if applicable. A customer might be a home user, an industrial plant, or a building. In addition to the meter, the customer domain interacts with the utility through the Energy Services Interface (ESI), which might communicate with additional domains through the Advanced Metering Infrastructure (AMI). A customer might also generate and store energy for transmission back into the Grid.

Advanced Metering Infrastructure

An important subsystem of the Smart Grid that is part of the customer domain in [Figure 4-1](#) is the AMI. The AMI comprises hardware and meter data management (MDM) software that provide the normal meter reading functions and support two-way communications that can exchange energy information and commands with customers' devices through a home area network. The AMI can be used to implement dynamic electricity pricing and load management, including voluntary programs where a customer can schedule load reductions with prior notice in return for pricing reductions. There are analogous networks that apply to the industrial customer.

In addition to the smart meter, another critical component of the AMI is the ESI, which acts as a gateway to the customer's network. While the smart meter provides functions, such as determining and communicating energy usage, connecting or disconnecting service, measuring the amount of power fed into the grid from distributed power sources, and communicating with the home area network or equivalent, the ESI serves as the connection to the energy service provider. The service provider is usually a utility, but it can also be a third party that provides energy management services to the customer.

Some of the functions that can be supported by the AMI include:

- Providing the ability of external, third-party clients to communicate with and control customer devices to allow

customers to take part in load reduction options

- Supporting voluntary load reduction at the customer's location by providing the customer with instantaneous kWhr electricity pricing
- Measuring the effectiveness of the voluntary load reduction incentives to the customer
- Optimizing building loads through building automation systems for large customers
- Providing the ability to detect, map, and restore outages to the customer

NIST⁶ identifies the following Smart Grid elements as participating in the AMI:

- Regional Transmission Organization (RTO) – An independent organization that coordinates, controls, and monitors the operation of the electrical power system and supply in a particular geographic area; similar to Independent System Operator
- Independent System Operator (ISO) – An independent entity that controls a power grid to coordinate the generation and transmission of electricity and ensure a reliable power supply
- Energy Market Clearinghouse – Wide-area energy market operation system providing high-level market signals for operations
- Service Provider – A person or company combining two or more customers into a single purchasing unit to negotiate the purchase of electricity from retail electric providers or the sale of electricity to these entities; providing consolidated bills to customers
- Utility Energy Management Systems (EMS) – The entities that continue to provide regulated services for the distribution of electricity (and gas and water) to customers and to serve customers that do not choose direct access. Regardless of where a customer chooses to purchase power, the customer's current utility will deliver the power to the customer's home or business.
- Operations – Calculation and analysis of power flow/state estimation results with the inclusion of distribution automation capabilities, demand response signaling, distributed energy resources, electric storage, PEVs (plug-in electric vehicles), and load management; provide a Web site

to enable customer access to usage and billing records

- Meter Data Management System (MDMS) – System providing meter data validation and verification so that reliable information can be used at bill settlement
- Metering System – The system used for collecting metering information
- Load Management System (LMS) – Controlling demand responses (DR), distributed energy resources (DER), plug-in electric vehicles (PEV), energy storage (ES) charging/discharging, processing and storing data on load management programs, storing information on contracts and relevant historic information, creating behavioral models, collecting, processing, and storing customer-specific power quality and reliability characteristics, and so on.
- Customer Information System (CIS) – Repository of customer information related to distribution company services. CIS contains load data for customers that are estimated for each nodal location on a feeder, based on billing data and time-of-day and day-of-week load shapes for different load categories.
- SCADA – SCADA database is updated via remote monitoring and operator inputs. Required scope, speed, and accuracy of real-time measurements are provided; supervisory and closed-loop control is supported.
- Field Devices – Field equipment with local intelligence for monitoring and control of automated devices in the distribution, which communicates with SCADA as well as distributed intelligence capabilities for automatic operations in a localized distribution area based on local information and on data exchange between members of the group.
- Meter – Unless otherwise qualified, a device of the utility used in measuring watts, vars, var-hours, volt-amperes, or volt-ampere-hours. Var stands for volt-ampere reactive power, which is the power in an AC circuit where there is a capacitive or inductive load.
- Energy Services Interface (ESI) – Provides cybersecurity and (often) coordination functions that enable secure interactions between relevant home area network devices and the utility. Permits applications such as remote load control, monitoring and control of distributed generation, in-home display of customer usage, reading of nonenergy meters, and integration with building management systems. Provides auditing/logging functions that record transactions to and from home area networking devices. Can also act as a gateway.
- Customer EMS – Customer energy management system that can

receive pricing and other signals for managing customer devices, including appliances, DER, electric storage, and PEVs.

- Customer Appliances, DER, PEV, and Electric Storage – Equipment and systems at the customer site that could participate in demand response and other programs
- Submeter – A meter that measures a subload, such as a plug-in electric vehicle.

Energy Storage and Management of Stored Energy

Energy storage (ES) is an important element of the Smart Grid concept. It can support the use of intermittent renewable energy devices and energy storage devices at the generating site, as well as allow for the use of electricity generated at a customer site. The connection of ES devices to the Grid must be done according to specified standards and guidelines to ensure the safe and efficient connection of external generation and storage devices to the Grid. These standards and guidelines have to address the following issues:

- Accommodation of intermittent renewable energy sources by storage of energy generated
- Effective deployment of ES-distributed energy resource (DER) systems
- ES-DER transmission implementations
- Interfaces to rotating machines
- Interoperability among ES-DER systems
- Modification of existing standards such as IEEE 1547⁷ to address various types of ES-DER systems and the DER connections with the Grid
- New Smart Grid storage and power electronics technologies

There are quite a few energy storage technologies being developed and/or improved that can be used in the Smart Grid architecture. Some of the more promising approaches are:

- Compressed Air – Energy is stored by pumping compressed air into a storage container or underground cavity and then releasing it when needed to power a turbine that generates electricity. An advantage is that it is a well-known technology, but a disadvantage is that it does impact the environment and requires a lengthy approval process. Compressed-air projects are used in large utility applications, but can be used in smaller applications.

- Flywheels – Energy is stored in large, high-mass, rapidly rotating discs, which can impart energy to generators to provide back-up or storage power and also support frequency regulation.
- Fuel Cells – Fuel cells produce electricity through conversion of chemical energy. A fuel cell requires a fuel supply and an oxidizing agent. A hydrogen fuel cell uses hydrogen as the fuel and oxygen as an oxidizer. Fuel cells can rapidly recharge.
- Lithium-ion Batteries – Modern technology battery with higher charging rates and higher energy densities than lead acid batteries. Development is focused on the automotive and electrical grid markets. These batteries have fast response and are best used at the generation project level.
- Pumped Hydro – Water is pumped from a lower-level storage basin to one at a higher level. Electricity can then be generated at a later time by having the water flow downhill through a turbine to generate electricity. This technology is used for centralized, utility-scale projects and is able to handle load with quick response.
- Sodium Sulfur Batteries – Batteries using sodium and liquid sulfur. These batteries are more efficient in larger sizes but have to be properly sealed and protected from water as sodium spontaneously explodes when it comes in contact with water.
- Ultracapacitors – Large amounts of electrical charge can be stored on new technology capacitors and then tapped when energy is needed. Capacitors typically have short charging times and provide high quantities of energy when discharged.

Smart Grid Protocols

The Smart Grid is a system of systems with two types of flow: power and communications. For data to be exchanged among all the domains of the Smart Grid, standard protocols must be used. There are a number of viable candidate protocols, each with its own advantages and disadvantages. One major candidate protocol is the Internet Protocol (IP), which was discussed in [Chapter 1](#).

IP was originally designed to allow dissimilar networks to communicate with each other and to provide flexibility in the types of physical connections used. It is widely deployed and has a base of support tools and security mechanisms. IP and the Internet protocols provide the advantages of interoperability with other applications that have been developed and deployed over the years relating to the Internet.

To be effective in the Smart Grid, a protocol must meet the requirements of

different domains of the Grid. For example, in the AMI, data collection does not have to be instantaneous and data can be collected every 15 or 20 minutes. Conversely, in the bulk generation facilities, operations have to be performed on the order of milliseconds. Thus, IP would be a good fit for the Smart Grid in general, but where deterministic elements are involved, other protocols more appropriate to control systems should be employed.

An additional standard that has been developed for interfacing to data communication networks, such as used in the Smart Grid, is defined in ANSI C12.22-2008⁷. ANSI C12.22 specifies a protocol for communicating with devices, such as data modules and meters. It provides security through the use of AES encryption methods. For Smart Grid purposes, ANSI C12.22 is an improvement over previous standards C12.18 and C12.21, which addressed meter reading through optical ports and modems, respectively, which are more suited to high-volume commercial and industrial customers. ANSI C12.22 is more appropriate for reading residential meters than C12.18 and C12.21. The main features of C12.22 are a protocol for the data link, physical layers for meter communications, and an application level protocol that is independent of the transport method used.

Another important protocol suite that is widely used in Europe in conjunction with smart meters is the IEC 62056-XX series. It is based on the Device Language Message Specification (DLMS)/Companion Specification for Energy Metering (COSEM) suite. DLMS uses the abstract modeling of communication elements, and COSEM establishes rules for smart meter data exchanges. DLMS/COSEM provides interoperability among a variety of meters and other modules. The components of the IEC 62056 series are summarized as follows:

- IEC 62056-21 – Defines data communications through electrical and optical ports
- IEC 62056-31 – Provides guidance on the use of local area networks on twisted pair
- IEC/TS 62056-41 – Addresses data communications over wide area networks
- IEC 62056-42 – Addresses physical layer services for asynchronous data interchanges
- IEC 62056-46 – Covers the High Level Data Link Control (HDLC) protocol for use in the data link layer
- IEC 62056-47 – Focuses on the COSEM IPv4 transport layer and communications from the application layer
- IEC/TS 62056-51 – Addresses protocols in the application layer
- IEC/TS 62056-52 – Discusses protocols for the management distribution line message specification (DLMS) server

- IEC 62056-53 – Provides guidance on establishing application associations among peer applications and messaging services
- IEC 62056-61 – Supports data identification for various types of data, including abstract data
- IEC 62056-62 – Defines the COSEM interface classes for modeling the range of meter functions

Mapping of Emerging Technology Issues onto an Example Automation System – The Smart Grid

The technologies associated with home area networks, energy storage, analytics, cloud computing, privacy, social networks, mobile technology, and interoperability will have a significant impact on industrial automation and control systems. [Figure 4-2](#) summarizes the domains of the Smart Grid that will be most affected by these technologies.

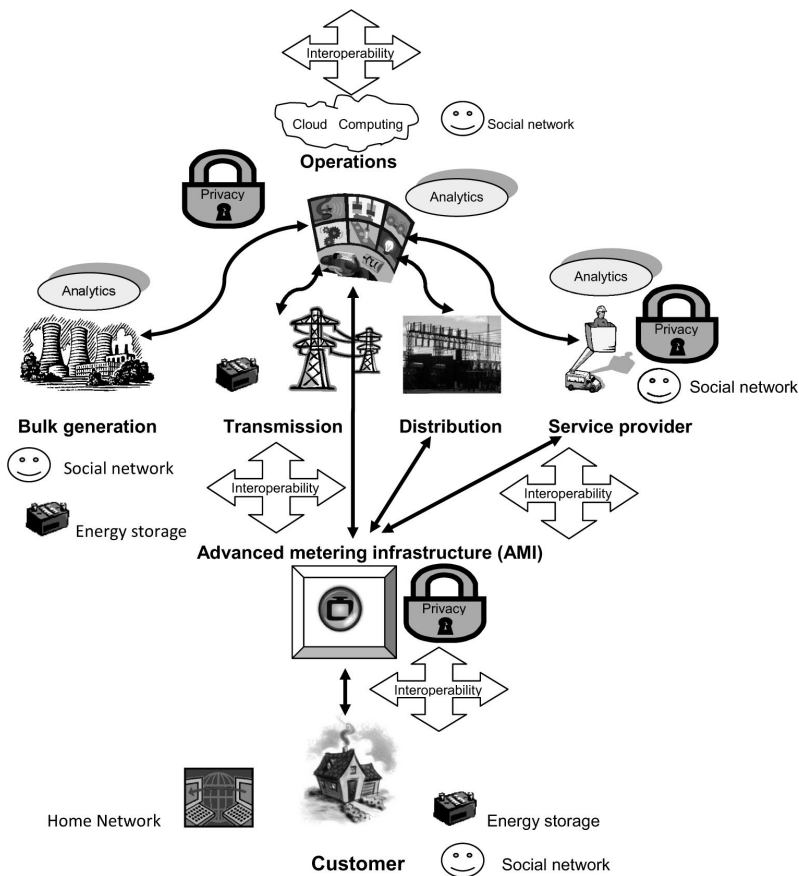


Figure 4-2. Smart Grid domains

To recap the earlier discussion:

Applying analytics in bulk generation can lead to improved and more efficient maintenance strategies by alerting operators before outages occur. In addition, the information obtained from applying analytics can lead to significant reductions in fuel costs, thus increasing profitability. Bulk generation facilities also require efficient and cost-effective energy storage, particularly for intermittent renewable energy sources, such as wind farms and solar collectors.

Social networking by operators with other domains can improve cooperation and understanding; however, it also holds the potential for compromise of sensitive information.

The transmission domain must maintain close communications with the operations domain and provide energy management and storage as needed. The distribution domain must also communicate with the operations domain and effectively provide electricity to the customer.

The service provider domain handles large amounts of customer personally identifiable information and must ensure that adequate privacy protections are in place. Social networking used in this environment offers benefits but might also be a source of security and privacy breaches.

The operations domain must communicate effectively with the other domains and provide efficient and reliable power management. In performing its functions, the operations domain can apply analytics to provide insight into potential problem areas before they become critical and can be used to initiate proactive solutions instead of reacting to system failures. With the large amount of data being gathered by the operations domain, cloud computing can offer significant value and savings by making on-demand applications and computing capacity available as needed. However, because social networking might also be involved in this domain, privacy protections have to be adequately implemented.

The AMI is a critical link to the customer domain and must ensure efficient transfer of information and offer privacy protections for PII.

The customer domain is the focus of all the other domains and can be a source or sink of electricity. It also provides communications with home area networks and smart meters to implement dynamic pricing and customer opt-in for energy savings. The customer domain, as a source of electricity to the Grid, can have energy storage capacity for intermittent sources of electricity. The customer domain can also have the highest volume of social networking and can thus be a source of compromise and loss of sensitive information.

All the domains must have high degrees of interoperability or the benefits of the Smart Grid will be significantly reduced.

Summary

Technological advancements pose a Cornelian dilemma in that choosing to use them or not to use them can both yield negative consequences. However, in most instances, the benefits of using them outweigh the risks. The key is to apply the new technologies in an intelligent and effective manner while implementing protections against the vulnerabilities introduced by these advancements.

Home area networks, energy storage, analytics, cloud computing, privacy, social networks, mobile technology, and interoperability can provide significant improvements in the performance, safety, security, and cost-effectiveness of industrial automation and control systems, if appropriate safeguards are employed.

Chapter 5 will explore the threats and risks to industrial automation and control systems and provide methods to quantify, evaluate, and manage the risks.

Review Questions for Chapter 4

1. Which of the following is an important element in connecting to smart meters?
 - a. Home area network
 - b. Energy storage devices
 - c. Cloud computing
 - d. Printers
2. Energy storage devices are especially useful in which of the following cases?
 - a. Fossil fuel energy sources
 - b. Nonrenewable energy sources
 - c. Intermittent renewable energy sources
 - d. Constant energy sources
3. The application of data mining and analysis to large amounts of data for the purposes of discovering knowledge and making intelligent predictions and decisions is known as which of the following?
 - a. Artificial intelligence
 - b. Analytics
 - c. Data aggregation
 - d. Predictive calculus
4. Which of the following techniques is used for condition monitoring of high voltage electrical equipment and identifying areas of potential failure?
 - a. Analytics

- b.Artificial intelligence
- c.Robotics
- d.Scanning

5.Data from a variety of sources that is analyzed in real time or near real time to perform predictive modeling and support physical, logical, and administrative security is known as which of the following?

- a.Data aggregation
- b.Cyber analytics
- c.Cybersecurity
- d.Sensitivity analysis

6.What of the following is NOT a characteristic of cloud computing?

- a.Measured service
- b.Resource pooling
- c.On-demand self-service
- d.Minimal elasticity

7.Which of the following is NOT one of the three cloud service models?

- a.Cloud application as a service
- b.Cloud software as a service
- c.Cloud platform as a service
- d.Cloud infrastructure as a service

8.Which of the following is NOT one of the five basic privacy principles?

- a.Access
- b.Choice
- c.Preemption
- d.Notice

9.Which of the following items is NOT one of the European Union (EU) privacy principles?

- a.Data should be collected in accordance with the law.

- b.Data should be used only for the purposes for which it was collected, and it should be used only for a reasonable period of time.
- c.Transmission of personal information to locations where equivalent personal data protection cannot be assured is permitted.
- d.Individuals have the right to correct errors contained in their personal data.

10.The ability of an entity to exchange information with another entity is known as which of the following?

- a.Compatibility
- b.Commonality
- c.Interchangeability
- d.Interoperability

11.Which of the following is NOT a distinguishing characteristic of the Smart Grid?

- a.Development and incorporation of demand response, demand-side resources, and energy efficiency resources
- b.Deployment and integration of distributed resources and generation, excluding renewable resources
- c.Provision to consumers of timely information and control options
- d.Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid

12.Which of the following is NOT an expected result of Smart Grid implementation?

- a.Higher grid resiliency
- b.Improved energy delivery efficiency
- c.Reduced operating costs
- d.Possible loss of customers

13.Which of the following is NOT a domain in the NIST Smart Grid framework?

- a.Control
- b.Customer
- c.Operations
- d.Bulk generation

14.Which domain of the Smart Grid framework provides energy generated from sources such as coal, gas, water from dams, nuclear reactions, geothermal, the sun, and wind?

- a.Distribution
- b.Transmission
- c.Bulk generation
- d.Service provider

15.Which domain of the Smart Grid delivers electrical power to the distribution domain and balances the required electrical load?

- a.Transmission
- b.Service provider
- c.Operations
- d.Bulk generation

16.Which domain of the Smart Grid handles customer problems and manages business accounts?

- a.Markets
- b.Service provider
- c.Markets
- d.Operations

17.What subsystem of the Smart Grid comprises hardware and meter data management (MDM) software that provide the normal meter reading functions as well as supporting two-way communications that can exchange energy information and commands with customer's devices through a home area network?

- a.Advanced Metering Infrastructure (AMI)
- b.Energy Management System (EMS)
- c.Energy Services Interface (ESI)

d.Smart Grid Interface (SGI)

18.In Smart Grid Terminology, DER stands for which of the following terms?

- a.Delayed energy reduction
- b.Determined energy requirements
- c.Distributed energy requirements
- d.Distributed energy resources

19.Which domain of the Smart Grid framework has a home area network and also might have a requirement for energy storage for intermittent sources of electricity?

- a.Customer
- b.Distribution
- c.Operations
- d.Markets

20.Which domain of the Smart Grid framework handles large amounts of customer personally identifiable information and must ensure that adequate privacy protections are in place?

- a.Customer
- b.Markets
- c.Service provider
- d.Operations

21.Which of the following evolving technologies can increase communications, collaboration, and innovation, but also be a source of compromise of PII and other sensitive information?

- a.Social networks
- b.Interoperability
- c.Cloud computing
- d.Analytics

22.Which domain of the Smart Grid framework does not have an energy storage requirement for intermittent sources of electricity?

- a.Customer

- b. Transmission
- c. Bulk generation
- d. Markets

23. Which domain of the Smart Grid framework has the most potential for benefiting from the use of cloud computing?

- a. Customer
- b. Transmission
- c. Distribution
- d. Operations

References

1 NIST SP 800-145 (Draft), *The NIST Definition of Cloud Computing (Draft)*, January 2011.

2 <http://newsroom.fb.com/Key-Facts/Statistics-8b.aspx>

3 Oladimeji, E. A., and Chung, L. "Analyzing Security Interoperability during Component Integration" in Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (July 10–12, 2006). ICIS-COMSAR, IEEE Computer Society, Washington, DC, pp. 121–129.

4 Office of the National Coordinator for Smart Grid Interoperability, NIST Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, January 2010.

5 The Smart Grid Interoperability Panel – Cybersecurity Working Group, NISTIR 7628, *Guidelines for Smart Grid Cybersecurity: Vol. 1, Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*, August 2010.

6 Office of the National Coordinator for Smart Grid Interoperability, NIST Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, January 2010.

7 IEEE 1547, *Standard for Interconnecting Distributed Resources with Electric Power Systems*, 2003.

Chapter 5

Risk Management for Industrial Automation and Control Systems

Chapter 4 explored the technological changes affecting industrial automation and control systems and their impact on securing such systems. Chapter 5 will develop the methodologies for identifying and mitigating risks in automation and control systems and provide the foundation for implementing security controls in Chapter 6.

Risk Management

Identifying and managing risks to industrial automation and control systems is a critical undertaking and a fundamental activity that is necessary to ensure the safety and security of these systems. ANSI/ISA-99.00.01-2007¹ defines risk as the “expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence.” Additional, important definitions from ANSI/ISA-99.00.01-2007 are:

- Threat – Potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm
- Vulnerability – Flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s integrity or security policy
- Residual risk – Remaining risk after the security controls or countermeasures have been applied
- Risk assessment – Process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure
- Risk management – Process of identifying and applying countermeasures commensurate with the value of the assets

protected based on a risk assessment

To obtain another perspective, NIST Special Publication 800-39² defines risk as “a measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” The other NIST SP 800-39 corresponding definitions are:

- Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service
- Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source
- Risk assessment – The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system
- Risk management – The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

The *Common Criteria*³ document describes the relationships among threats, risk, countermeasures, and assets to be protected, as shown in [Figure 5-1](#).

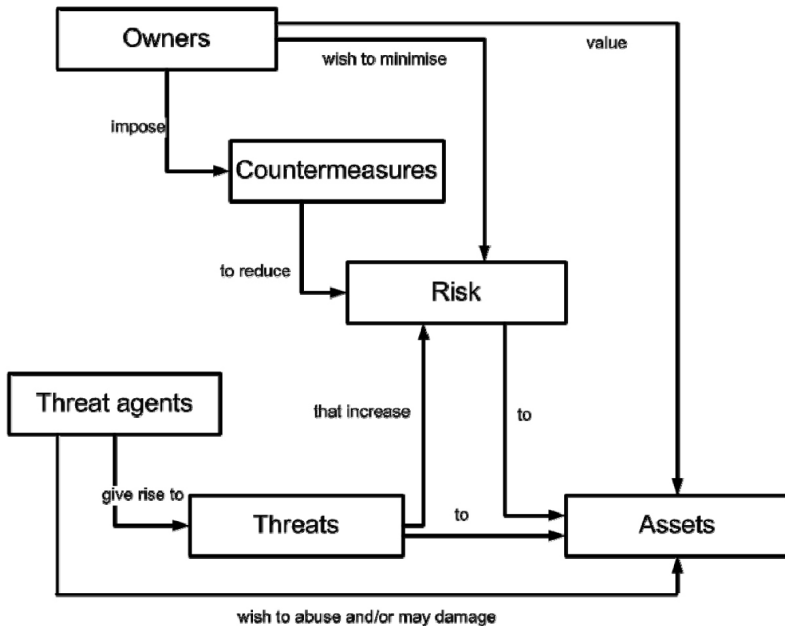


Figure 5-1. Risk relationships

[Source: *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model*, Version 3.1, Revision 3, July 2009.]

Assets can include physical elements, such as computer hardware, control systems, or specialized equipment, in addition to intangible assets, such as intellectual property, compliance information, or process expertise. Another important category of asset is the individual or professional who professes unique knowledge and skills that, for example, are critical in the operation and maintenance of industrial automation and control systems.

Three valuable approaches to risk management are presented in ANSI/ISA-99.02.01-2009, NIST SP 800-39, and NIST SP 800-37, which will be reviewed in the following sections.

ANSI/ISA-99.02.01 Cybersecurity Management System

To determine and mitigate risk, ANSI/ISA-99.02.01-2009⁴ defines a cybersecurity management system (CSMS) as shown in Figure 5-2.

The CSMS comprises the three main categories of risk analysis, addressing the risk, and monitoring and improving the CSMS.

Risk Analysis

In the risk analysis category of the CSMS, a business rationale is established, and risk identification, classification, and assessment are conducted. The business rationale includes the following:

- Establishing a basis for securing the industrial automation and control system
- Obtaining management support for securing the automation and control system
- Identifying and understanding the consequences of a successful attack on the automation and control system

Risk identification, classification, and assessment include ascertaining and prioritizing the risks to industrial automation and control systems and estimating the likelihood and impact of those risks. Specifically, this area of the CSMS includes the following activities:

- Select a risk assessment methodology
- Conduct a high-level risk assessment
- Identify the industrial automation and control systems to be addressed
- Develop simple network diagrams
- Prioritize the systems for mitigation
- Perform a detailed vulnerability assessment
- Conduct a detailed risk assessment
- Maintain vulnerability assessment records

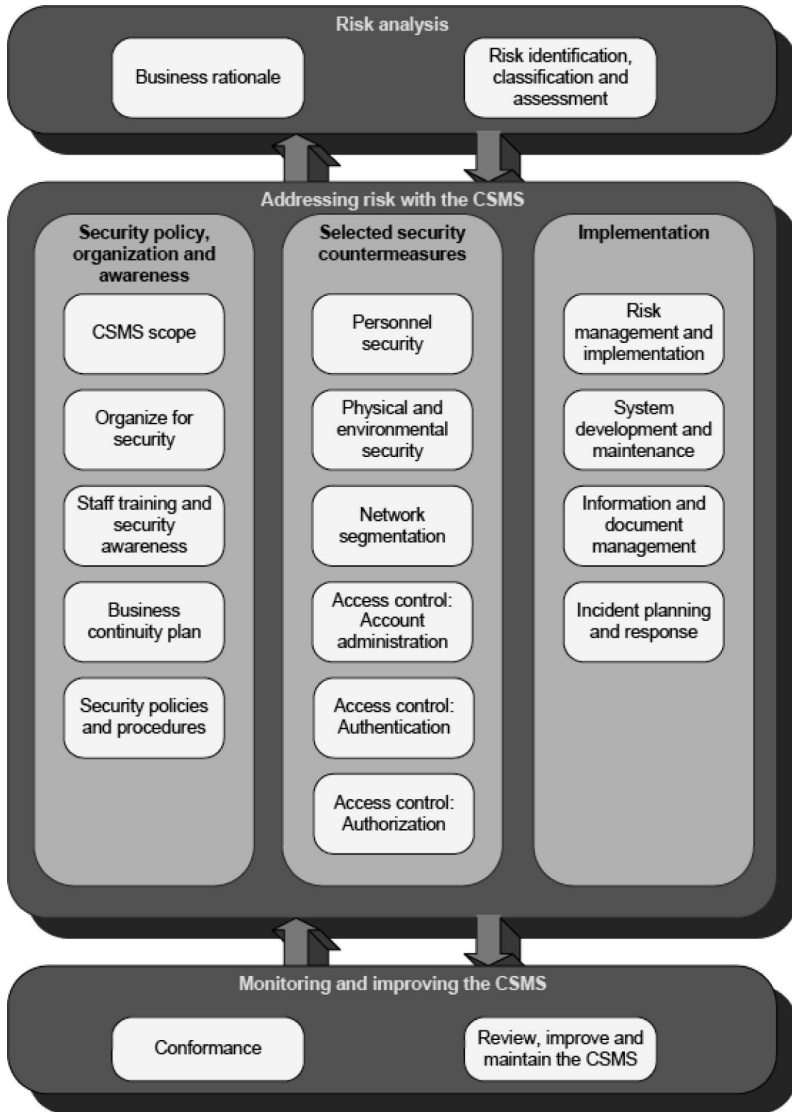


Figure 5-2. Cybersecurity management system (CSMS)

[Source: ANSI/ISA-99.02.01-2009 n 3.1, Revision 3, July 2009.]

Addressing Risk

The next major CSMS category, addressing risk, comprises the following areas:

- Security policy, organization and awareness
- Selected security countermeasures
- Implementation

As shown in [Figure 5-2](#), security policy, organization and awareness includes documenting the elements that fall within the scope of the CSMS and assigning responsibilities for overall cybersecurity. In addition, this category incorporates providing staff and contractor personnel with adequate training and information to be aware of threats and weaknesses, and to have the ability to take remedial action if necessary. Further activities include developing a business continuity plan for reestablishing essential business operations upon the occurrence of an event that causes a business disruption and developing security policies and procedures applicable to automation and control systems and compatible with general organizational policies.

The second group under addressing risk with the CSMS is selected security countermeasures. The activities in this group include personnel security, physical and environmental security, network segmentation, and access control of account administration, authentication, and authorization.

Personnel security is concerned with evaluating personnel to ensure they exhibit appropriate behaviors and will be able to preserve the security of the automation and control systems.

Physical and environmental security are focused on protecting industrial automation and control systems from physical threats and malfunctions in environmental systems, such as power supplies and temperature controls.

In *network segmentation*, networks are subdivided into zones that have similar security requirements and characteristics, and they are separated by protective devices to screen traffic from one network segment to another.

Access control determines which entities can have access to resources; it is broken down into *account administration*, *authentication*, and *authorization*. In account administration, access to accounts is controlled and limited to entities that have privileges associated with those accounts. Authentication requires strong verification of a claimed user's identity prior to granting access to specific resources, and authorization provides access privileges to specific accounts upon successful authentication.

The third CSMS group under addressing risk is implementation, which comprises risk management and implementation, system development and maintenance, information and document management, and incident planning and response.

Risk management and implementation consist of identifying and putting in place countermeasures that are technically and financially warranted to address determined risks. *System development and maintenance* emphasizes the inclusion of cybersecurity considerations throughout the system development life cycle, including in the maintenance phase when system changes might frequently occur. *Information and document management* is concerned with applying information and document management policies in order to protect sensitive information from unauthorized disclosure. The last item in this group, *incident planning and response*, focuses on having plans and procedures in place to effectively respond to incidents, including reporting and investigative and follow-up activities.

Monitoring and Improving the CSMS

The last category of the CSMS, monitoring and improving the CSMS, consists of the elements of (a) conformance and (b) review, improve, and maintain the CSMS. *Conformance* verifies that an automation and control system is compliant with appropriate policies, procedures, and regulations. *Review, improve, and maintain the CSMS* requires continuous supervision of the CSMS to make sure responses to changes or threats are incorporated into the CSMS.

An additional benefit of implementing a CSMS, as cited in ANSI/ISA-99.00.01-2007⁵, is maintaining the security level of industrial automation and control systems over time. Many security efforts are undertaken on a project basis, and system security deteriorates over time with the evolution of new threats and changes in the system architecture. Figure 5-3 illustrates the relative security levels of project-oriented industrial automation and control systems (IACS) and CSMS-based IACS.

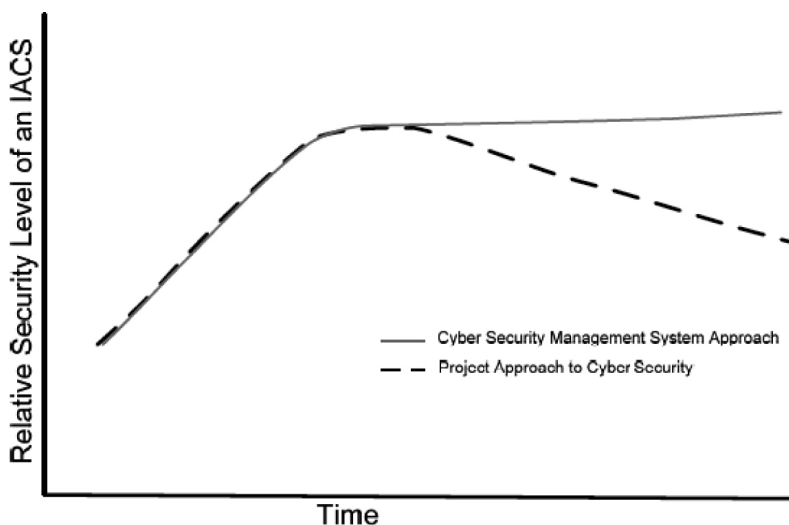


Figure 5-3. Relative cybersecurity over time

NIST Special Publication 800-39 Integrated Enterprise Risk Management

NIST SP 800-39⁶, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011 replaces NIST SP 800-30⁷, *Risk Management Guide for Information Technology Systems*, which, at the time of writing, is being revised to provide guidance on risk assessment as a supporting document to Special Publication 800-39. NIST SP 800-39 views risk management as:

A comprehensive process that requires organizations to:
(i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis, using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.

Toward these ends, it takes a global view of risk management and does not limit the risk management process to elements of information systems or automation and control systems alone. The approach views risk management as a hierarchical structure that has to involve the organization's mission and business goals, the organization's business processes, and the system development life cycle of information and automation system components. The document formalizes these subject areas into the following three tiers:

- Tier 1 – Organization: Establishes and implements governance structures consistent with organizational mission and goals
- Tier 2 – Mission/Business Processes: Designs, develops, and implements mission/business processes to support the mission defined in Tier 1
- Tier 3 – Information Systems: Integrates risk management activities into the system development life cycle (SDLC) of organizational information systems and addresses the resilience of organizational information systems. Tier 3 risk is addressed through NIST SP 800-53, which incorporates security controls for automation systems. These controls will be discussed in detail in [Chapter 6](#).

This multitiered approach is summarized in [Figure 5-4](#).

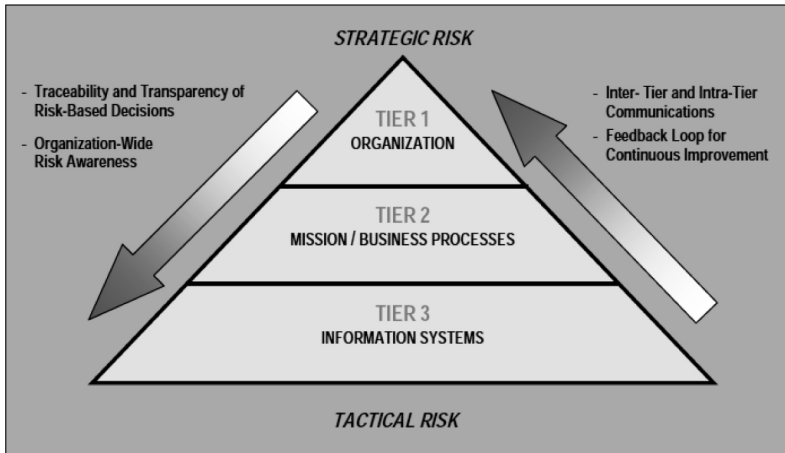


Figure 5-4. Multitiered risk management

[Source: NIST SP 800-39, March 2011.]

In [Figure 5-4](#), Tier 1 risk management prioritizes mission/business functions, evaluates strategic and funding alternatives, provides risk management guidance to authorizing officials, and establishes the order of recovery of critical information systems.

Tier 2 execution follows from the output of Tier 1 activities. Tier 2 functions include defining the necessary and critical mission/business processes of the organization, prioritizing these functions based on organizational objectives, and determining the specific types of information necessary to carry out the organization's mission/business processes. An important concept in Tier 2 is the information security architecture, which is that part of the enterprise architecture that is concerned with the robustness of the information or automation and control system and its resistance to attacks. The information security architecture should incorporate the best elements of defense in depth and defense in breadth and is illustrated in [Figure 5-5](#). Defense in breadth is a planned, systematic set of multidisciplinary activities that seek to mitigate risk at every stage of the system development life cycle.

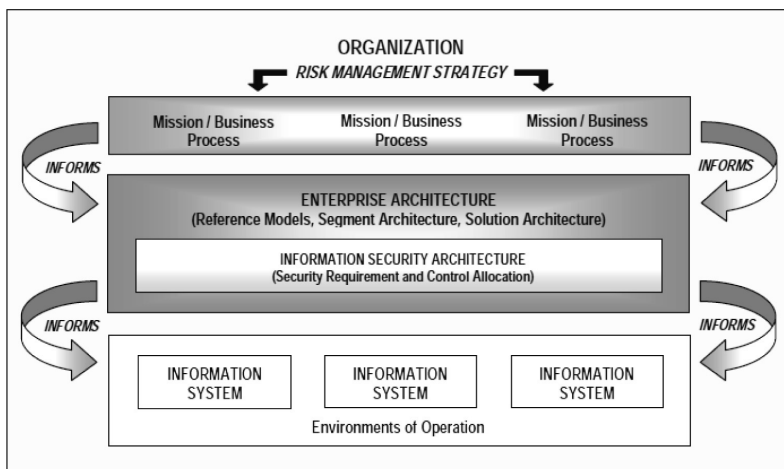


Figure 5-5. Integration of information security requirements

[Source: NIST SP 800-39, March 2011.]

Figure 5-5 shows that risk management can be addressed as an element of the enterprise architecture. The process is summarized in NIST SP 800-39 as:

- Developing a segment architecture linked to the strategic goals and objectives of organizations, defined missions/business functions, and associated mission/business processes
- Identifying where effective risk response is a critical element in the success of organizational missions and business functions
- Defining the appropriate, architectural-level information security requirements within organization-defined segments based on the organization's risk management strategy
- Incorporating an information security architecture that implements architectural-level information security requirements
- Translating the information security requirements from the segment architecture into specific security controls for information systems/environments of operation as part of the solution architecture
- Allocating management, operational, and technical security controls to information systems and environments of operation as defined by the information security architecture
- Documenting risk management decisions at all levels of the enterprise architecture

Tier 3 focuses on information systems or automation and control systems and follows from the information passed down from tiers 1 and 2. Some tier 3 functions include categorizing organizational information systems, properly allocating security controls to those systems to support the organization's mission/business processes, and managing and monitoring security controls on an ongoing basis. Tier 3 addresses risk management in the following system development life cycle phases, which includes that of industrial automation and control systems:

- 1.Initiation
- 2.Development/acquisition
- 3.Implementation
- 4.Operations/maintenance
- 5.Disposal

As defined above, NIST SP 800-39 defines the components of risk management as risk framing, risk assessment, risk response, and risk monitoring. The relationship of these components to the three tiers is given in [Figure 5-6](#).

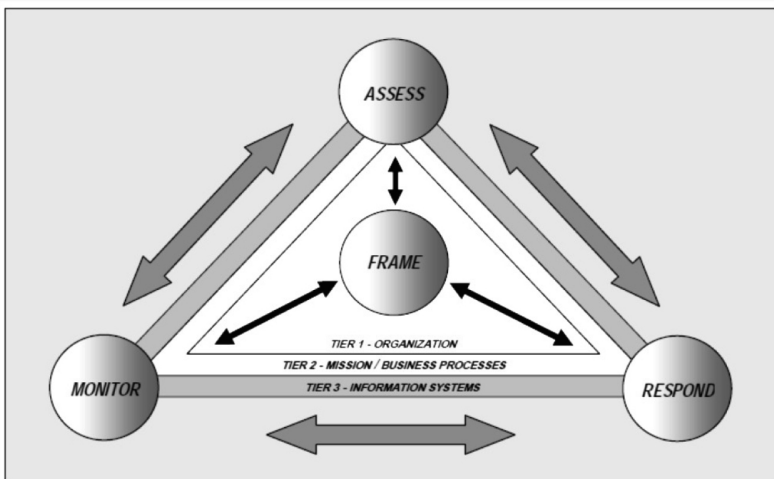


Figure 5-6. Risk management and the tiers

[Source: NIST SP 800-39, March 2011.]

Risk framing ([Figure 5-6](#)) includes the following tasks:

1. Making assumptions about threats, vulnerabilities, consequences/impact, and likelihood of occurrence
2. Determining restraints on risk assessment, response, and monitoring
3. Determining risk tolerance levels
4. Identifying priorities and trade-offs

Risk assessment includes the following activities:

1. Identifying threats to the organization
2. Identifying vulnerabilities
3. Determining the impact of threats realized
4. Determining the likelihood of harm occurring

Risk response includes:

1. Developing alternative courses of action
2. Evaluating these alternative courses of action
3. Selecting the best courses of action
4. Implementing selected responses

Risk monitoring is concerned with:

1. Confirming that risk response measures have been implemented
2. Evaluating the effectiveness of implemented risk response measures
3. Determining changes to organizational information systems that would affect risk

NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems

NIST SP 800-37⁸ provides additional risk management guidance through the Risk Management Framework (RMF), which “provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF operates primarily at Tier 3 in the risk management hierarchy, but can also have interactions at Tiers 1 and 2.” The RMF comprises the following elements:

- Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- Select** an initial set of baseline security controls for the information system based on the security categorization, tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and on local conditions.
- Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.
- Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the nation, resulting from the operation of the information system and the decision that this risk is acceptable.
- Monitor** the security controls in the information system on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

The Insider Threat

As discussed in the previous ANSI and NIST documents in this chapter, one of the major efforts in risk management is to determine the threats to an industrial automation and control system. Most conventional threats have been reviewed extensively in many books and papers. One important conventional threat that deserves attention is the insider attack. This type of attack, from individuals within an organization, is of particular concern because it can bypass many institutional safeguards. Some of the common characteristics of insider attacks are:

- Many attacks are conducted by a disgruntled insider.
- In common with other types of attacks, insider attacks make systems unavailable and can result in serious losses and harm to reputation.

- Insiders who initiate attacks against computers usually give some indication of dissatisfaction beforehand.
- Many insider attacks are conducted remotely.
- Most inside attackers have privileged access to computer systems.
- Many insider attacks are planned in advance.

Threat Examples Worthy of Note

A number of threats are so potentially harmful that it is important to look at them as learning examples and as a means to understand how to counteract threats in general.

There are two threats to industrial automation and control systems that are out of the ordinary and worthy of detailed exploration. These threats are Stuxnet and electromagnetic pulse (EMP) emanations.

Stuxnet and Defensive Approaches

Stuxnet is a worm that was designed to change control outputs on specific PLCs and conceal its existence from control room observers. It is of such complexity that it is probably the product of a team of programmers working many months to develop, debug, and test. The sophistication of Stuxnet leads many to believe it is the product of one or more nations working together. Some of the salient characteristics of Stuxnet are:

- Discovered in June 2010, but suspected to have been spread many months before
- Infects Windows PCs
- Modifies WinCC databases, which provide process visualization HMI functions
- Attacks both networked and non-networked PCs
- Accomplishes infection through USB flash drives
- Uses zero-day exploits, which take advantage of previously unidentified vulnerabilities
- Installs device drivers, using valid, digital certificates “appropriated” from trusted sources
- Specifically targets Siemens SIMATIC STEP 7 PLCs through a Windows PC
- Manipulates output bits on PLCs that control processes

- Focuses, it is speculated, on disrupting the operation of centrifuges at the Iranian Natanz uranium enrichment facility by changing values on turbine controls and frequency converters
- Receives updates through communications with servers in Denmark and Malaysia and through peer-to-peer communications
- Conceals its actions from the network control center so that operators do not have any indication of improper operations or malfunctions

From the information known about Stuxnet, it is not a great leap to imagine it being targeted at elements of a nation's critical infrastructure, particularly the Smart Grid, in addition to refineries, chemical plants, pipelines, and so on.

Preventive measures against Stuxnet include scanning and using firewalls on both incoming and outgoing connections to control the spread of the worm to other systems. However, because Stuxnet launched a zero-day attack, which exploited heretofore unknown Microsoft vulnerabilities, it will be difficult to detect other possible intrusions taking advantage of future, unknown vulnerabilities.

A promising countermeasure against worms, such as Stuxnet, is the use of whitelisting of valid, executable code. In whitelisting, software that is "clean" and not compromised is placed on a "whitelist" and only that code can be run on the control system. The code is validated by generating a cryptographic hash or message digest from the code, and this value is stored for future reference. Then, whenever a program is scheduled for execution, its hash is generated and compared against the hash of the original "clean" program. If the hashes are identical, the code has not been modified and is permitted to run. If the hashes are different or there is no such hash on the valid hash list, then the code is marked as malware and is not executed. Whitelisting is, thus, effective against "zero-day" attacks in that this countermeasure is not dependent on knowing the signature of malicious code in advance.

One problem with whitelisting is that, in an environment where there are frequent changes and patches to software, the whitelist has to be constantly updated to keep current. Fortunately, most automation and control systems do not require as many updates as IT systems.

Another concept related to whitelisting is intrusion tolerance. Intrusion tolerance assumes that malicious attacks will succeed in penetrating a computing system and performs actions to negate their effects. A good example of intrusion tolerance is the Self Cleansing Intrusion Tolerance (SCIT)⁹ system developed by Professor Arun Sood of George Mason

University, colleagues, and students.

SCIT counters malware by repeatedly booting up a new, clean version of the operating system at predefined and selectable intervals. SCIT operates in the following manner:

1. When a server is booted, the SCIT control software launches a pristine, malware-free copy of the server's operating system into a virtual machine.
2. Following a random time period when the operating system has been exposed to the Internet, the virtual server is taken off-line and replaced by a clean, new, virtual server.
3. The removed server is then cleaned and loaded with a new, clean version of the operating system and placed in the queue for subsequent activation.

SCIT assumes that attacks are potentially always in progress and does not attempt to detect intrusions but continuously goes about replacing and cleaning the potentially corrupted software. [Figure 5-7](#) illustrates the on-line servers and the servers being cleaned. There is a continuous decommissioning and commissioning of servers at approximately 30-second intervals.

An SCIT virtual machine can be in one of the following four states:

1. Active state – The virtual machine is running on-line and accepts and processes requests.
2. Grace period state – The virtual machine processes existing requests but does not service any new requests.
3. Inactive state – The virtual machine is not performing any tasks and is off-line for cleaning.
4. Live spare state – The virtual machine has been cleaned and is ready to return to on-line processing.

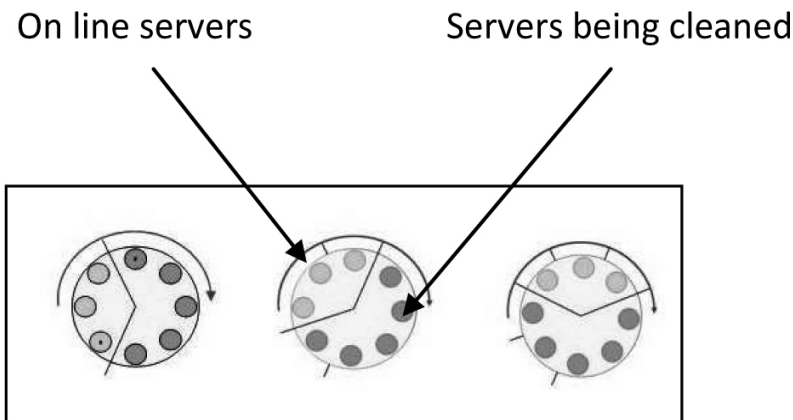


Figure 5-7. SCIT decommissioning and commissioning of virtual servers

[Source: *Securing Web Servers Using Self Cleansing Intrusion Tolerance (SCIT)*, Proceedings of the Second International Conference on Dependability, June 2009.]

An example application of SCIT to industrial automation and control systems might be in some of the domains of the Smart Grid, for example, the operations, service provider, or customer domain. In the customer domain, SCIT could be used in the Advanced Metering Infrastructure (AMI). SCIT would serve to prevent intrusions into the Smart Grid infrastructure through potentially vulnerable interfaces, such as in smart meters and data collection points.

Yet another, albeit more restrictive approach to protecting industrial automation and control systems is to limit the transmission of data to only one direction, from the automation and control system to the higher corporate IT system. In this manner, no malicious code can be sent from the IT-connected Internet to control systems. This method is known as a data diode in that it allows data to be transmitted in one direction only. The unilateral transmission of messages has obvious advantages, but its use is limited to architectures that do not rely on two-way transmission of data and commands. A number of data diode products are available that support a variety of automation and control system protocols.

Worms, such as Stuxnet, raise the specter of cyberwarfare among nations. This situation raises a number of difficult questions for dealing with such attacks. For example:

- Does the military have a role in defending against cyberattacks?
- How does one determine if the attack was initiated by a state or by rogue individuals operating in a state?

- How may the origin of a cyberattack be determined and with what accuracy?
- Is international law up-to-date with the technical progress of digital systems?
- Should preemptive attacks be used?
- Should the military role be offensive, defensive, or both?
- What part does international law play in cyberwarfare?

Electromagnetic Pulse

A threat not commonly planned for in industrial automation and control systems is electromagnetic pulse (EMP) interference. William Radasky, in a paper titled “High Power Electromagnetic (HPEM) Threats to the Smart Grid¹⁰,” analyzes this threat and its potential effects on power distribution systems. Because the Smart Grid depends more on electronic communication and processing resources, it can be more vulnerable to EMP than older power systems.

EMP can originate from the following three primary sources:

- A high-altitude nuclear detonation in space at heights above 30 km – High Altitude EMP (HEMP)
- Solar activity – Geomagnetic storms
- Electromagnetic emanations created by terrorists or criminal elements – Intentional Electromagnetic Interference (IEMI)

HEMP

As discussed in the “High Power Electromagnetic (HPEM) Threats to the Smart Grid” paper, HEMP has the following three time-based components:

- Early-time (E1) within 10 ns of the burst – Produces an electric field pulse in the range of 2.5 to 25 ns at levels of approximately 50 kV/m that travels at the velocity of light. This field can penetrate substation walls and induce voltages of around 20 kV into substation control circuits.
- Intermediate-time (E2) between 1 microsecond and 1 second after the burst – Produces field levels reaching 100 V/m
- Late-time (E3) between 1 second and several hundred seconds after the burst – Produces field levels reaching 40 V/km

It is estimated that the environments at times E1 and E3 have the potential of

causing the most damage to electric power systems because of the combination of high coupling efficiency to control lines and the peak field level values. Also, microwave towers with their extensive cabling are ideal induction targets for E1 HEMP, providing a path to sensitive communications and control equipment. E1 HEMP is also a serious threat to SCADA systems in power generation facilities, including controls and communications for wind turbines, solar cells, and other variable generation sources. E3 HEMP pulses are typically on the order of 1 second to several hundred seconds and can generate fields that are capable of coupling 4000 V between transformer grounded neutrals and inducing currents on the order of 800 A. This activity can also generate harmonics that would propagate through the power system and cause large amounts of damage, particularly to the equipment of the Smart Grid.

Solar

Regarding solar activity, extreme geomagnetic storms on the sun can generate electric fields in the range of 20 V/km and cause distortions in the Earth's surface geomagnetic field. Such changes cause fluctuations in the earth's electric field; these fluctuations induce currents in the neutral lines and generate damaging harmonics in the power grids, similar to E3 HEMP. On August 6, 2011, U.S. government scientists warned users of satellite, telecommunications, and electric equipment to prepare for possible disruptions occurring during the week. "The magnetic storm that is soon to develop probably will be in the moderate to strong level," said Joseph Kunches, a space weather scientist at the Space Weather Prediction Center, a division of the U.S. National Oceanic and Atmospheric Administration (NOAA). He stated that solar storms occurring during this period could affect communications and global positioning system (GPS) satellites and might even produce an aurora visible as far south as Minnesota and Wisconsin. Tom Bogdan, Director of the Center, said the sun is going from a quiet period into a busier cycle for solar flares, and an increase in the number of such blasts is expected over the next three to five years. Similarly, the Sunday, August 7, edition of *The New York Times*, in an article titled "Effects of Solar Flares Arriving on Earth," stated that "operators of electrical grids are working to avoid outages, but the National Oceanic and Atmospheric Administration says some satellite communications and global positioning systems could face problems."

IEMI

IEMI is categorized into wideband and narrowband fields above 100 MHz with peaks at 10 kV/m or higher. IEMI poses significant threats to substation electronics, smart meters, communications systems, and so on.

Protection

Protective measures cited by Radasky¹¹ against EMP threats include placing control rooms and electronics in basements surrounded by soil, which offers some protection against EMP fields. Cabling should also be placed in the

center of the building, if possible, to minimize EMP inductive fields.

- EM shielding should be applied to protect vulnerable electronics in control centers and power generating facilities.
- Fiber optic cabling can minimize coupling if properly applied.
- High-frequency grounding with filters and surge arrestors can be used to protect sensors, smart meters, communications systems, and so on.

Protection against EMP should take into account the following field characteristics:

- High-frequency pulses can induce currents in floating wires.
- High-frequency pulses can penetrate through windows and gaps in metal shields.
- High-frequency fields do not have high energy content and therefore, surge protection devices can be effective.
- Low-frequency electromagnetic fields, such as those generated by E3 HEMP and extreme geomagnetic storms, can be mitigated by incorporating good grounding techniques and by using capacitors on neutral connections to provide a fast bypass mechanism for surges.

Some organizations and standards that address EMP threats include:

- IEC SC 77C - *EMC: High Power Transient Phenomena and Smart Grid Implications*
- IEEE P1642 The IEEE EMC Society/TC-5 (High-power EM), *Recommended Practice for Protecting Public Accessible Computer Systems*
- IEEE/ANSI C62.41 *Product Application Location, Test Methods, Guide to Using the Standard*
- MIL-STD 188-125-1 *HEMP Hardening (Fixed Facilities)*
- MIL-STD 188-125-2 *HEMP Hardening (Transportable Systems)*
- MIL-STD 202 *Environmental Requirements Component Level*
- MIL-STD 461 *EMI Requirements (Subsystems)*
- MIL-STD 464 *EMI Requirements (Systems)*
- MIL-STD 810 *Environmental Requirements Box Level*

- RTCA DO-160F *Aircraft Protection*
- The International Council on Large Electric Systems WG C4.206 *Protection of the High Voltage Power Network Control Electronics against Intentional Electromagnetic Interference (IEMI)*
- The International Telecommunications Union (ITU-T) Study Group 5
- UL1449 *Safety Standards for Low Voltage Surge Protective Devices* (Steering Committee)

Summary

Chapter 5 discussed and summarized three important risk management methodologies and their application to industrial automation and control systems. A key component of risk management is risk mitigation, and, in developing this topic, this chapter provides a basis for Chapter 6. In Chapter 6, approaches and means to secure industrial automation and control systems are developed along with guidelines for maintaining that security.

Review Questions for Chapter 5

1. In ANSI/ISA-99.00.01-2007, a “potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm,” is which of the following?
 - a. Threat
 - b. Vulnerability
 - c. Weakness
 - d. Risk
2. The “expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence” is which of the following?
 - a. Consequence
 - b. Threat source
 - c. Weakness
 - d. Risk
3. The program and supporting processes to manage information security risk

to organizational operations (i.e., mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation are defined as which of the following?

- a.Risk assessment
- b.Risk management
- c.Risk mitigation
- d.Risk association

4.Which of the following is considered an asset in risk management?

- a.Computer hardware
- b.A control system
- c.A professional with unique knowledge
- d.All of the above

5.The ANSI/ISA-99.02.01-2009 Cybersecurity Management System (CSMS) comprises which of the following three main categories?

- a.Risk analysis, addressing the risk, and monitoring and improving the CSMS
- b.Risk mitigation, addressing the risk, and monitoring and improving the CSMS
- c.Risk analysis, addressing the risk, and monitoring and improving the automation system
- d.Risk analysis, eliminating the risk, and monitoring and improving the CSMS

6.In the CSMS, a business rationale is established. Which of the following is NOT one of the elements of the business rationale?

- a.Establishing a basis for securing the industrial automation and control system
- b.Obtaining management support for securing automation systems
- c.Identifying and understanding the consequences of a successful attack on automation systems
- d.Confirmation of the value of the automation system

7.The risk identification, classification, and assessment activities of the CSMS

do NOT include which of the following?

- a. Conduct a high-level risk assessment
- b. Develop simple network diagrams
- c. Mitigate the risk
- d. Perform a detailed vulnerability assessment

8. Which of the following is NOT one of the areas included in “Addressing risk with the CSMS?”

- a. Security policy, organization and awareness
- b. Correction
- c. Selected security countermeasures
- d. Implementation

9. Subdividing a network into zones that have similar security requirements and characteristics and are separated by protective devices to screen traffic from one network segment to another is known as which of the following?

- a. Network segmentation
- b. Network isolation
- c. Network masking
- d. Network fragmentation

10. In the CSMS, access control is subdivided into which of the following three areas?

- a. Account verification, authentication, and authorization
- b. Account administration, authentication, and authorization
- c. Account administration, audit, and authorization
- d. Account administration, authentication, and activation

11. Risk management, system development and maintenance, and incident planning are part of which of the following areas of addressing risk in the CSMS?

- a. Security policy, organization, and awareness
- b. Selected security countermeasures

c.Implementation

d.Scope

12.In the monitoring and improving category of the CSMS, which element verifies that an automation system is compliant with appropriate policies, procedures, and regulations?

a.Review

b.Conformance

c.Improve

d.Maintain

13.NIST SP 800-39 views which of the following as a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis?

a.Risk management

b.Risk assessment

c.Risk monitoring

d.Risk evaluation

14.NIST SP 800-39 defines three tiers. Which of the following include those three?

a.Policy, Mission/Business Processes, Information Systems

b.Organization, Policy, Information Systems

c.Organization, Mission/Business Processes, Objectives

d.Organization, Mission/Business Processes, Information Systems

15.Categorizing organizational information systems and properly allocating security controls to those systems to support the organization's mission/business processes is performed in which tier of the multitiered risk management architecture?

a.Tier 1

b.Tier 2

c.Tier 3

d.Tier 4

16.According to NIST SP 800-39, risk framing, risk assessment, risk response, and risk monitoring are components of which of the following?

- a.Risk valuation
- b.Risk determination
- c.Risk management
- d.Risk acceptance

17.Making assumptions about threats, vulnerabilities, consequences/impact, and likelihood of occurrence are part of which of the following, according to NIST SP 800-39?

- a.Risk assessment
- b.Risk framing
- c.Risk response
- d.Risk monitoring

18.Which of the following is NOT an element of responding to risk, according to NIST SP 800-39?

- a.Evaluating the effectiveness of implemented risk response measures
- b.Developing alternative courses of action
- c.Selecting the best courses of action
- d.Implementing selected responses

19.According to NIST SP 800-37, which of the following “provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle?”

- a.Risk Monitoring Framework (RMF)
- b.Risk Assessment Framework (RAF)
- c.Risk Management Framework (RMF)
- d.Risk Evaluation Framework (REF)

20.Which of the following groups of elements is presented in NIST SP 800-37 to manage risk?

- a.Categorize, Select, Implement, Authorize
- b.Categorize, Evaluate, Implement, Monitor
- c.Determine, Select, Implement, Authorize
- d.Determine, Evaluate, Implement, Monitor

21.Which of the following is NOT characteristic of an insider threat?

- a.Many insider attacks are conducted by disgruntled insiders
- b.Most insider attacks do not result in serious losses or harm
- c.Many insider attacks are conducted remotely
- d.Many inside attackers have privileged access to computer systems

22.Which of the following best describes Stuxnet?

- a.A worm that was designed to change control outputs on specific PLCs and conceal its existence from control room observers
- b.A worm that was designed to modify email messages and conceal its existence from control room observers
- c.A virus that was designed to modify disk storage and send random messages to users' computers
- d.A virus that was designed to crash computers when email attachments were opened

23.Which of the following is NOT true regarding Stuxnet?

- a.Attacks both networked and non-networks PCs
- b.Installs device drivers using valid, digital certificates
- c.Infects Apple Macintosh computers
- d.Infection is accomplished through USB flash drives

24.The process that only uses software that is “clean” and not compromised and is verified before running is known as which of the following?

- a.Confirming
- b.Whitelisting
- c.Cleanlisting

d.Prechecking

25.An electromagnetic pulse generated by a high-altitude nuclear detonation in space at heights above 30 km is known as which of the following?

- a.Intentional Electromagnetic Interference (IEMI)
- b.Space Generated EMP (SGEMP)
- c.Intensive Electromagnetic Interference (IEMI)
- d.High Altitude EMP (HEMP)

26.Which one of the following is NOT a component of a High Power Electromagnetic (HPEM) burst?

- a.Final-time (E4) – Several hundred seconds after the burst
- b.Early-time (E1) – Within 10 ns of the burst
- c.Intermediate-time (E2) – Between 1 microsecond and 1 second after the burst
- d.Late-time (E3) – Between 1 second and several hundred seconds after the burst

27.Solar-generated EMP is the result of which of the following actions?

- a.Changes in the sun's orbit
- b.Solar eclipses
- c.Geomagnetic storms on the sun
- d.Changes in the earth's orbit

28.Which of the following statements is NOT true regarding EMP?

- a.High-frequency pulses can induce currents in floating wires.
- b.High-frequency pulses can penetrate through windows and gaps in metal shields.
- c.High-frequency grounding with filters and surge arrestors can be used to protect sensors, smart meters, and communications systems.
- d.Fiber optic cabling cannot minimize coupling.

References

- 1 ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, October 2007.
- 2 NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
- 3 ISO/IEC 15408, *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model*, Version 3.1, Revision 3, July 2009.
- 4 ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, January 2009.
- 5 ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, October 2007.
- 6 NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
- 7 NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.
- 8 NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010.
- 9 Bangalore, A. and Sood, A. *Securing Web Servers Using Self Cleansing Intrusion Tolerance (SCIT)*, Proceedings of the Second International Conference on Dependability (DEPEND 2009), June 2009.
- 10 Radasky, W. "High Power Electromagnetic (HPEM) Threats to the Smart Grid," *Interference Technology, 2011 EMC Directory and Design Guide*, 2011.
- 11 Radasky, W. "High Power Electromagnetic (HPEM) Threats to the Smart Grid," *Interference Technology, 2011 EMC Directory and Design Guide*, 2011.

Chapter 6

Industrial Automation and Control Systems Security Methodologies and Approaches

Chapter 5 presented important risk management methodologies and their application to industrial automation and control systems. Chapter 6 will build on the results of risk management and develop in detail the foundation of security controls that are proven, effective, and applicable to industrial automation and control systems.

Automation and Control System Security Standards and Guidelines

The fundamental principles for protecting computer systems and networks are valid across all application domains. However, these principles have to be tailored to the world of industrial automation and control systems to be effective in protecting these systems. From experience and application of engineering approaches, a number of standards and guidelines have been developed and documented for securing automation and control systems. These materials take in to account the characteristics of industrial automation and control systems and present measures that should be taken to protect these systems.

Some of the important documents that address automation and control system security are:

- NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*
- ANSI/ISA-TR99.00.01-2007, *Security Technologies for Industrial Automation and Control Systems*
- North American Electric Reliability Corporation (NERC), *Critical Infrastructure Protection (CIP) Cybersecurity Standards*

- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*
- Department of Homeland Security, *Catalog of Control Systems Security: Recommendations for Standards Developers*
- AMI-SEC Task Force, *AMI System Security Requirements*
- DOD Instruction 8500.2, *Information Assurance (IA) Implementation*

This list is not meant to be all-inclusive, but it comprises some of the major standards and guidelines addressing industrial automation and control system security and, among them, covers the major protection approaches to securing these systems. These standards and guidelines will be explored in this chapter. Following this exposition, the controls described will be cross-correlated in a table to provide a concise summary of these protection mechanisms with references back to the authoritative document.

NIST Special Publication 800-82, *Guide to Industrial Control Systems Security*

NIST SP 800-82¹ defines the major objectives for an industrial control system (ICS) security implementation as the following:

- Restricting logical access to the ICS network and network activity.** This includes using a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks, and having separate authentication mechanisms and credentials for users of the corporate and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Restricting physical access to the ICS network and devices.** Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.
- Protecting individual ICS components from exploitation.** This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services; restricting ICS user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls, such as antivirus software and file integrity checking

software, where technically feasible to prevent, deter, detect, and mitigate malware.

- Maintaining functionality during adverse conditions.** This consists of designing the ICS so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, and does not cause another problem elsewhere, such as a cascading event.
- Restoring system after an incident.** Incidents are inevitable and an incident response plan is essential. A major characteristic of a good security program is how quickly a system can be restored after an incident has occurred.

NIST SP 800-82 categorizes recommended security controls into management controls, operational controls, and technical controls.

Management Controls

Management controls consist of risk assessment, planning, system and services acquisition, certification, accreditation, and security assessments.

Risk assessment is defined in NIST SP 800-82 as “the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.” NIST SP 800-39, *Managing Information Security Risk*, and NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, provide guidance in the application of risk assessment, as discussed in [Chapter 5](#).

The remaining management controls are summarized as follows:

- Planning** is the generation of a plan to determine and implement security controls, perform assessments, conduct incident response, and assign security levels. Continuous security evaluations and upgrades should be provided for through the security life cycle, keeping in mind the characteristics of industrial automation and control systems. The security life cycle integrates information security into the system development life cycle.
- System and services acquisition** is the process of generating risk assessment-based acquisition policies and providing resources that address automation and control system security through the system development life cycle, including external suppliers. The systems life cycle comprises (i) initiation, (ii) development/acquisition, (iii) implementation, (iv)

operation/maintenance, and (v) disposal.

- Certification, accreditation, and security assessments** have the goals of ensuring that the specified controls are properly implemented and functioning as desired. A senior organizational official is responsible for accepting residual risk, and all security controls should be regularly monitored. Certification and accreditation are required for government agencies and Department of Defense entities, but equivalent evaluations can be performed for industrial automation and control systems.

Operational Controls

Operational controls are those controls that are performed by personnel as opposed to computer systems. NIST 800-82 defines these controls as follows:

- Personnel Security (PS):** policies and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security
- Physical and Environmental Protection (PE):** policies and procedures addressing physical, transmission, and display access control as well as environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, fire protection)
- Contingency Planning (CP):** policies and procedures designed to maintain or restore business operations, including computer operations (possibly at an alternate location) in the event of emergencies, system failures, or disaster
- Configuration Management (CM):** policies and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure that the automation and control system is protected against improper modifications prior to, during, and after system implementation
- Maintenance (MA):** policies and procedures to manage all maintenance aspects of an automation and control system
- System and Information Integrity (SI):** policies and procedures to protect information systems and their data from design flaws and data modification, using functionality verification, data integrity checking, intrusion detection, malicious code detection, and security alert and advisory controls
- Media Protection (MP):** policies and procedures to ensure secure handling of media. Controls cover access, labeling, storage, transport, sanitization, destruction, and disposal
- Incident Response (IR):** policies and procedures pertaining to

incident response training, testing, handling, monitoring, reporting, and support services

- Awareness and Training (AT):** policies and procedures to ensure that all information system users are given appropriate security training, relative to their use of the system, and that accurate training records are maintained

Technical Controls

Technical controls are characterized by implementation through software, hardware, or firmware elements. Based on NIST 800-53², NIST 800-82 defines the following technical controls:

- Identification and Authentication (IA):** the process of verifying the identity of a user, process, or device through the use of specific credentials (e.g., passwords, tokens, biometrics) as a prerequisite for granting access to resources in an IACS
- Access Control (AC):** the process of granting or denying specific requests for obtaining and using information and related information processing services for physical access to areas within the IACS environment
- Audit and Accountability (AU):** independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures
- System and Communications Protection (SC):** mechanisms for protecting both system and data transmission components

The application of these management, operational, and technical controls will serve to reduce the risk to industrial automation and control systems and will mitigate vulnerabilities. Another perspective, which reinforces the controls of NIST 800-82, includes the controls recommended by ANSI/ISA-TR99.00.01-2007.

ANSI/ISA-TR99.00.01-2007, Security Technologies for Industrial Automation and Control Systems

ANSI/ISA-TR99.00.01-2007³ provides information on a variety of cybersecurity technologies for industrial automation and control systems (IACS). This data can be used to mitigate risk and improve the security posture of industrial automation and control systems. The controls of ANSI/ISA-TR99.00.01-2007 are organized into the following categories:

- Authentication and Authorization Technologies
- Filtering/Blocking/Access Control Technologies
- Encryption Technologies and Data Validation
- Management, Audit, Measurement, Monitoring, and Detection Tools
- Industrial Automation and Control Systems Computer Software
- Physical Security Controls

Authentication and Authorization

ANSI/ISA-TR99.00.01-2007 describes authorization as “the initial step in protecting an IACS system and its critical assets from unwanted breaches. It is the process of determining who and what should be allowed into or out of a system.” Authentication is defined as “the process of positively identifying potential network users, hosts, applications, services, and resources, using a combination of identification factors or credentials. The result of this authentication process then becomes the basis for permitting or denying further actions.” In addition, authentication is further divided into the following two areas:

- User Authentication** – Traditional computer authentication, such as “logging into a computer” or activating a human-machine interface (HMI) to adjust a process
- Network Service Authentication** – The ability for networked devices to distinguish between authorized and unauthorized remote requests for IACS data or to perform actions on the IACS

The major components of authentication and authorization technologies spelled out in ANSI/ISA-TR99.00.01-2007 are summarized as follows:

- Role-based Authorization** – Role-based access control (RBAC) uses roles, hierarchies, and constraints to organize user access levels and is attractive in situations where employees change positions frequently in an organization.
- Password Authentication** – These technologies authenticate an individual, using a secret known by the user, such as a password or PIN. ANSI/ISA-TR99.00.01-2007 points to an issue to be considered in a control environment where, “during a major crisis when human intervention is critically required, an operator may panic and have difficulty remembering the password and either be locked out completely or delayed in being able to respond to the event. If

the password has been entered wrong and the system has a limit on allowed wrong password entries, the operator may be locked out permanently until an authorized employee can reset the account.”

- Challenge/Response Authentication** – This authentication method uses a challenge/response, which requires a requestor and service provider both to share a secret. A challenge is sent to the service provider, and it answers with a unique, expected response.
- Physical/Token Authentication** – The person requesting access uses a token or smart card, which might use multifactor authentication, to gain access to a system.
- Biometric Authentication** – Biometric authentication uses the biological characteristics of an individual to confirm his or her identity. Characteristics include fingerprints, retina signatures, facial recognition, and signature dynamics.
- Location-Based Authentication** – The authentication of a requestor is based on his or her physical location, as determined by a GPS or IP address.

Filtering/Blocking Access Control

This control uses filtering/blocking access control technologies, such as firewalls. A firewall provides for tracking successful and unsuccessful transmissions through the firewall, restricting data entering or leaving a network, and supporting interactions among networks. A firewall can filter by applications, ports, or IP addresses.

Specifically, ANSI/ISA-TR99.00.01-2007 states:

Firewalls enforce access control policies using mechanisms that either block or permit certain types of traffic, thus regulating the flow of information. Firewalls typically block traffic from the outside of a protected area to the inside of a protected area, while permitting users on the inside to communicate with outside services. While it is important to have a firewall separating a company's enterprise network from the Internet, it is even more important to have firewalls between the enterprise network and industrial automation and control systems LANs.

The three primary types of firewalls are summarized as follows:

- Packet Filtering** – Evaluates the address information in each

packet of data relative to certain criteria and, as a result, can either drop the packet, forward the packet, or send a message to the originator. It looks at the data packet to get information about the source and destination addresses, the session's communications protocol (TCP, UDP, or ICMP), and the source and destination application port for the desired service. Because the processing of packets in this type of firewall requires a small amount of overhead, it has minimal impact on system performance.

- Stateful Inspection** – Filters packets at the network layer, determines whether session packets are valid, and evaluates the packet at the application layer. A stateful inspection firewall uses an inspection engine to extract state-related information. This information includes packet sequence numbers, IP addresses, and ports engaged in the connection. It maintains this information in a dynamic state table and evaluates subsequent connection attempts. This type of firewall offers a high level of security, good performance, and transparency to end users, but is relatively expensive.
- Application Proxy** – Is commonly a host computer that is running proxy server software, making it a proxy server. It operates by transferring a copy of each accepted data packet from one network to another, thereby masking the data's origin. A proxy server can control which services a workstation uses on the Internet, and it aids in protecting the network from outsiders who may be trying to get information about the network's design. This type of firewall is also called an application layer gateway. It offers a high level of security but has a significant impact on network performance.

Encryption Technologies Data Validation

Symmetric and asymmetric encryption technologies (detailed in [Chapter 2](#)) are used to protect sensitive process-related information. Data validation technologies safeguard the accuracy and completeness of information used in the industrial process. As stated in ANSI/ISA-TR99.00.01-2007, “Symmetric key encryption can be used to distinguish communication by devices that are not part of the desired network. This feature is generally attractive for SCADA and other process control systems that wish to allow little or no access to the control network, but is difficult to deploy in systems requiring unrestricted Internet access.” Encryption can also be employed in a virtual private network (VPN), which provides for authentication, integrity, and protection from unauthorized disclosure. The most common VPN implementations are Internet Protocol Security (IPSec), Secure Shell (SSH), and Secure Sockets Layer (SSL).

Management, Audit, Measurement, Monitoring, and Detection

Audit and related mechanisms are used to evaluate the security posture of an industrial automation and control system, and forensic methods are used to detect and analyze incidents. Some of the events that can be tracked in typical audit and logging environments for automation systems are:

- Access to files, folders, or other resources
- Account logon events to automation system elements
- Changes to specific accounts
- Directory service accesses
- Instances of elevated privileges to specific users or accounts
- Process accesses
- Security policy modifications
- System events

Regarding management issues, ANSI/ISA-TR99.00.01-2007 discusses host configuration management (HCM) tools that systems administrators use to manage resources centrally, control access to systems, and set a general level of security for each host on a network. However, it notes that “industrial automation and control systems do not typically use HCM tools because of the policy-driven nature of the tools. Most of the configuration is done through the IACS application and is established because of functional needs rather than administrative or security policies.”

Other management aids, automated software management (ASM) tools, are applications used to distribute software across a network to specified hosts or groups of hosts. They are employed, to some degree, in IACS applications and are used to manage updates to antivirus and firewall software, for application version control, and for patch management.

Industrial Automation and Control Systems Computer Software

Automation and control system software might contain vulnerabilities due to programming errors and should be tested and evaluated to eliminate any such risk factors. ANSI/ISA-TR99.00.01-2007 identifies the three main types of software that have to be considered in industrial automation and control systems as server and workstation operating systems, real-time and embedded operating systems, and Web servers and Internet technologies. Many automation and control system hosts and HMI computers use the Windows, Unix, and Linux operating systems and are therefore vulnerable to attacks designed for these systems. Real-time devices and controllers, in many cases, use specific, vendor developed operating systems.

Physical Security Controls

These controls are defined by ANSI/ISA-TR99.00.01-2007 as “any physical measures, either active or passive, that limit physical access to any information assets in the IACS environment.” Physical security devices are designed to protect computer media assets and documents, physical equipment assets, personnel, and facilities. The three main categories of physical security control devices are:

- Active** – Active devices are devices that can be engaged or disengaged as a function of policy, time, control algorithms, or other input. Typical examples are gates, locks, movable barriers, and doors.
- Identification and Monitoring Devices** – These devices include various types of cameras, recording devices, sensors, and biometric devices. They usually require monitoring by a human to make security decisions.
- Passive** – Passive devices are hard installations, such as concrete barriers, fences, and walls.

Personnel Security Controls

In ANSI/ISA-TR99.00.01-2007, personnel security falls under the category of physical security, and its elements are hiring policies, terms and conditions of employment, and related company policies and practices.

North American Electric Reliability Corporation, Critical Infrastructure Protection Cybersecurity Standards

The North American Electric Reliability Corporation (NERC) *Critical Infrastructure Protection (CIP) Cybersecurity Standards*⁴ (<http://www.nerc.com/page.php?cid=2|20>) are divided into Standards CIP-002-4 through CIP-009-4 and address “the identification and protection of critical cyber assets to support reliable operation of the Bulk Electric System (BES).” These eight standards will be reviewed in the following sections with the purpose of highlighting the important automation and control system security controls used in electricity generation and distribution systems. Even though these CIP standards were designed for the electric utility industry, the security principles listed are sound and applicable to the manufacturing and process industries. In particular, the following requirements, explained in detail in the following paragraphs, are particularly useful to enhancing the security of automation systems:

- CIP-002-4 - R1, R2

- CIP-003-4 - R4, R5, R6
- CIP-004-4 - R1, R2, R3
- CIP-005-4 - R1, R2, R3, R4, R5
- CIP-006-4 - R1, R2, R5
- CIP-007-4 - R1, R2, R3, R4, R8
- CIP-008-4 - R1
- CIP-009-4 - R1, R2

CIP-002-4 Cybersecurity – Critical Cyber Asset Identification

Standard CIP-002-4 requires the responsible entity to identify and document the critical cyber assets associated with the respective bulk electric system. The standard sets forth the following requirements for critical asset identification:

R1. Critical Asset Identification – The responsible entity shall develop a list of its identified critical assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The responsible entity shall update this list as necessary and review it at least annually. (Author note: Attachment 1 comprises items such as generating facilities, reactive power resources, blackstart resources, and transmission facilities.) The term blackstart refers to restarting a power system after all or part of the system has shut down. The restarting is implemented by isolated power stations being started individually and gradually being reconnected to each other in order to form an interconnected system again.

R2. Critical Cyber Asset Identification – Using the list of critical assets developed pursuant to Requirement R1, the responsible entity shall develop a list of associated critical cyber assets essential to the operation of the critical asset. The responsible entity shall update this list as necessary and review it at least annually.

For the purpose of Standard CIP-002-4, critical cyber assets are further qualified to be those having at least one of the following characteristics:

- The cyber asset uses a routable protocol to communicate outside the electronic security perimeter.

- The cyber asset uses a routable protocol within a control center.
- The cyber asset is dial-up accessible.

R3. Annual Approval – The senior manager or delegate(s) shall approve annually the list of critical assets and the list of critical cyber assets. Based on Requirements R1 and R2, the responsible entity may determine that it has no critical assets or critical cyber assets. The responsible entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of critical assets and the list of critical cyber assets (even if such lists are null.)

Standard CIP-002-4 considers the following to be critical assets with numbering as in the standard:

1.1 Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net real power capability of the preceding 12 months equal to or exceeding 1500 MW in a single interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation facilities) having aggregate net reactive power nameplate rating of 1000 mega volt Amperes Reactive (MVAR) or greater.

1.3. Each generation facility that the planning coordinator or transmission planner designates and informs the generator owner or generator operator as necessary to avoid Bulk Electric System (BES) adverse reliability impacts in the long-term planning horizon.

1.4. Each blackstart resource identified in the transmission operator's restoration plan.

1.5. The facilities comprising the cranking paths and meeting the initial switching requirements from the blackstart resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the cranking path where two or more path options exist, as identified in the transmission operator's restoration plan. A cranking path is defined as a portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units.

1.6. Transmission facilities operated at 500 kV or higher.

1.7. Transmission facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission facilities at a single station or substation location that are identified by the reliability coordinator, planning authority, or transmission planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the reliability coordinator, planning authority, or transmission planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any generator owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission facilities identified as essential to meeting nuclear plant interface requirements.

1.12. Each special protection system (SPS), remedial action scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing under voltage load shedding (UVLS) or under frequency load shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the reliability coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation facility or group of generation facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the transmission operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the balancing authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the balancing authority for generation equal to or greater than an aggregate of 1500 MW in a single interconnection.

CIP-003-4 Cybersecurity – Security Management Controls

Standard CIP-003-4 requires that “Responsible Entities have minimum security management controls in place to protect critical cyber assets.” The specific requirements as given in CIP-003-004 are summarized as follows:

R1. Cybersecurity Policy – The responsible entity shall document and implement a cybersecurity policy that represents management’s commitment and ability to secure its critical cyber assets.

R2. Leadership – The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to, standards CIP-002-4 through CIP-009-4.

R3. Exceptions – Instances where the responsible entity cannot conform to its cybersecurity policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R4. Information Protection – The responsible entity shall implement and document a program to identify, classify, and protect information associated with critical cyber assets.

R5. Access Control – The responsible entity shall document and

implement a program for managing access to protected critical cyber asset information.

R6. Change Control and Configuration Management – The responsible entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing critical cyber asset hardware or software and implement supporting configuration management activities to identify, control, and document all entity or vendor-related changes to hardware and software components of critical cyber assets pursuant to the change control process.

CIP-004-4 Cybersecurity – Personnel & Training

Standard CIP-004-4 requires that “personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.”

The requirements of CIP-004-4 are:

R1. Awareness – The responsible entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to critical cyber assets receive ongoing reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer-based training)
- Indirect communications (e.g., posters, intranet, brochures)
- Management support and reinforcement (e.g., presentations, meetings)

R2. Training – The responsible entity shall establish, document, implement, and maintain an annual cybersecurity training program for personnel having authorized cyber or authorized unescorted physical access to critical cyber assets. The cybersecurity training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R3. Personnel Risk Assessment – The responsible entity shall have a documented personnel risk assessment program, in accordance

with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to critical cyber assets. A personnel risk assessment shall be conducted pursuant to that program, prior to such personnel being granted such access, except in specified circumstances, such as an emergency.

R4. Access – The responsible entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets.

CIP-005-4 Cybersecurity – Electronic Security Perimeter(s)

Standard CIP-005-4 addresses “the identification and protection of the electronic security perimeter(s) inside which all critical cyber assets reside, as well as all access points on the perimeter.” The requirements for this standard are summarized as follows:

R1. Electronic Security Perimeter – The responsible entity shall ensure that every critical cyber asset resides within an electronic security perimeter. The responsible entity shall identify and document the electronic security perimeter(s) and all access points to the perimeter(s).

R2. Electronic Access Controls – The responsible entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter(s).

R3. Monitoring Electronic Access – The responsible entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the electronic security perimeter(s) twenty-four hours a day, seven days a week.

R4. Cyber Vulnerability Assessment – The responsible entity shall perform a cyber vulnerability assessment of the electronic access points to the electronic security perimeter(s) at least annually.

R5. Documentation Review and Maintenance – The responsible entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.

CIP-006-4 Cybersecurity – Physical Security of Critical Cyber Assets

The CIP-006-4 standard “is intended to ensure the implementation of a physical security program for the protection of critical cyber assets.” A summary of the requirements of this standard is given as follows:

R1. Physical Security Plan – The responsible entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All cyber assets within an electronic security perimeter shall reside within an identified physical security perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the responsible entity shall deploy and document alternative measures to control physical access to such cyber assets.

R1.2. Identification of all physical access points through each physical security perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4, including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a physical security perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from physical security perimeters.

R1.6.2. Continuous escorted access of visitors within the physical security perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems – cyber assets that authorize and/or log access to the physical security perimeter(s), exclusive of hardware at the physical security perimeter access point, such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

R3. Protection of Electronic Access Control Systems – cyber assets used in the access control and/or monitoring of the electronic security perimeter(s) shall reside within an identified physical security perimeter.

R4. Physical Access Controls – The responsible entity shall document and implement the operational and procedural controls to manage physical access at all access points to the physical security perimeter(s) twenty-four hours a day, seven days a week.

R5. Monitoring Physical Access – The responsible entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the physical security perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4.

R6. Logging Physical Access – Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The responsible entity shall implement and document the technical and procedural

mechanisms for logging physical entry at all access points to the physical security perimeter(s).

R7. Access Log Retention – The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R8. Maintenance and Testing – The responsible entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly.

CIP-007-4 Cybersecurity – Systems Security Management

Standard CIP-007-4 requires “responsible entities to define methods, processes, and procedures for securing those systems determined to be critical cyber assets, as well as the other (noncritical) cyber assets within the electronic security perimeter(s).” Because this standard describes the security controls for protecting the critical infrastructure, it is one of the most important in the CIP list. The recommendations of CIP-007-4 are summarized as follows:

R1. Test Procedures – The responsible entity shall ensure that new cyber assets and significant changes to existing cyber assets within the electronic security perimeter do not adversely affect existing cybersecurity controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The responsible entity shall create, implement, and maintain cybersecurity test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The responsible entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The responsible entity shall document test results.

R2. Ports and Services – The responsible entity shall establish, document, and implement a process to ensure that only those ports

and services required for normal and emergency operations are enabled.

R2.1. The responsible entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The responsible entity shall disable other ports and services, including those used for testing purposes, prior to production use of all cyber assets inside the electronic security perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the responsible entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management – The responsible entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document, and implement a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all cyber assets within the electronic security perimeter(s).

R4. Malicious Software Prevention – The responsible entity shall use antivirus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all cyber assets within the electronic security perimeter(s).

R5. Account Management – The responsible entity shall establish, implement, and document technical and procedural controls that enforce access authentication of and accountability for all user activity and that minimize the risk of unauthorized system access.

R6. Security Status Monitoring – The responsible entity shall ensure that all cyber assets within the electronic security perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cybersecurity.

R6.1. The responsible entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all cyber

assets within the electronic security perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected cybersecurity Incidents.

R6.3. The responsible entity shall maintain logs of system events related to cybersecurity, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The responsible entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The responsible entity shall review logs of system events related to cybersecurity and maintain records documenting review of logs.

R7. Disposal or Redeployment – The responsible entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of cyber assets within the electronic security perimeter(s) as identified and documented in Standard CIP-005-4.

R8. Cyber Vulnerability Assessment – The responsible entity shall perform a cyber vulnerability assessment of all cyber assets within the electronic security perimeter at least annually.

CIP-008-4 Cybersecurity – Incident Reporting and Response Planning

Standard CIP-008-4 “ensures the identification, classification, response, and reporting of cybersecurity Incidents related to critical cyber assets.” The associated requirements of the standard are the following:

R1. Cybersecurity Incident Response Plan – The responsible entity shall develop and maintain a cybersecurity incident response plan and implement the plan in response to cybersecurity incidents. The cyber-security incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable cybersecurity incidents.

R1.2. Response actions, including roles and responsibilities of cybersecurity incident response teams, cybersecurity

incident handling procedures, and communication plans.

R1.3. Process for reporting cybersecurity incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The responsible entity must ensure that all reportable cybersecurity incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the cybersecurity incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the cybersecurity incident response plan is reviewed at least annually.

R1.6. Process for ensuring the cybersecurity incident response plan is tested at least annually. A test of the cybersecurity incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cybersecurity Incident Documentation – The responsible entity shall keep relevant documentation related to cybersecurity incidents reportable per Requirement R1.1 for three calendar years.

CIP-009-4 Cybersecurity – Recovery Plans for Critical Cyber Assets

Standard CIP-009-4 “ensures that recovery plan(s) are put in place for critical cyber assets and that these plans follow established business continuity and disaster recovery techniques and practices.” The corresponding requirements are:

R1. Recovery Plans – The responsible entity shall create and annually review recovery plan(s) for critical cyber assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises – The recovery plan(s) shall be exercised at least

annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control – The recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore – The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore critical cyber assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup.

R5. Testing Backup Media – Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

NIST Special Publication 800-53, Revision 3, Recommended Security Controls for Federal Information Systems

NIST Special Publication 800-53⁵ provides a catalog of security controls that can be used to obtain compliance with requirements from governmental agencies, military services, and other sources. As stated in the document, “The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner—thus contributing to the organization’s confidence that there is ongoing compliance with its stated security requirements.” The publication was aimed originally at IT systems but now includes an appendix that addresses the application of the controls to industrial automation and control systems.

As of this writing, a draft of a newer version of NIST SP 800-53, revision 4, has been released for comments. In addition to addressing industrial automation and control systems, revision 4 includes a Privacy Control Appendix and addresses new areas, including:

- Application security
- Firmware integrity
- Distributed systems
- Advanced persistent threat
- Insider threat
- Mobile computing
- Cloud computing
- Application security
- Supply chain risk

The security controls in NIST SP 800-53, Revision 3, are divided into 18 families, each with a unique two-character identifier. The control families are themselves partitioned into three classes: management, operational, and technical. Table 6-1 lists the control identifiers and summarizes the control families and classes.

Table 6-1. NIST SP 800-53 Control families and classes

	Family
Technical Control	AC
Operations and Training	AT
Technical Accountability	ALP
Security Assessment and Authorization	CA
Configuration Management	CM
Operational Planning	CP
Identification and Authentication	IA
Incident Response	IR
Maintenance	MA
Media Protection	MP
Physical and Environmental Protection	PE
Management	PL
Personnel Security	PS
Risk Assessment	RA
Supply Chain Services Acquisition	SA
System and Communications Protection	SC
System Information Integrity	SI
Management	PM

[Source: NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, August 2009.]

The format of a typical SP 800-53 control is as follows:

SI-3 MALICIOUS CODE PROTECTION

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:

- Transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or
- Inserted through the exploitation of information system vulnerabilities;

b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

- Perform periodic scans of the information system [*Assignment: organization - defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
- [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]*] in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, Web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file.

Pervasive configuration management and strong software integrity controls may be effective in Special Publication 800-53 *Recommended Security Controls for Federal Information Systems and Organizations* preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyberattacks that could affect organizational missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Related controls: SA-4, SA-8, SA-12, SA-13, SI-4, SI-7.

Control Enhancements:

- (1) The organization centrally manages malicious code protection mechanisms.
- (2) The information system automatically updates malicious code protection mechanisms (including signature definitions).
- (3) The information system prevents nonprivileged users from circumventing malicious code protection capabilities.
- (4) The information system updates malicious code protection mechanisms only when directed by a privileged user.
- (5) The organization does not allow users to introduce removable media into the information system.
- (6) The organization tests malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing a known benign, nonspreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur as required.

References: NIST Special Publication 800-83.

The NIST SP 800-53 controls are considered baseline controls, which can be tailored to more closely meet the needs of a particular organization and automation systems. NIST SP 800-53 describes the tailoring process as follows:

1. Applying scoping guidance to the initial baseline security controls to obtain a preliminary set of applicable controls for the tailored baseline
2. Selecting (or specifying) compensating security controls, if needed, to adjust the preliminary set of controls to obtain an equivalent set deemed to be more feasible to implement
3. Specifying organization-defined parameters in the security controls via explicit assignment and selection statements to complete the definition of the tailored baseline

The scoping guidance referred to in item 1 of the tailoring process is designed to ensure that only the controls appropriate to the particular mission and requirements of the organization are used. Some factors to consider in scoping include:

- Are there common controls specified by the organization?
- What are the primary security objectives?
- To what system components are the controls applicable?
- What technologies are employed in the system (e.g., cryptography, wireless)?
- What are the policy and regulatory requirements?
- What is the operational environment?
- Are there scalability requirements?
- Is public access permitted?

NIST SP 800-53 provides for the use of compensating security controls, which the publication defines as “a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control ... that provides an equivalent or comparable level of protection for an information system and the information processed, stored, or transmitted by that system.”

Similarly, recognizing some of the special requirements of industrial automation and control systems, NIST SP 800-53 defines supplements to the baseline control systems to address automation and control system issues. These supplements are summarized in [Table 6-2](#).

Table 6-2. Industrial Control System Supplements

Control number

Control name

Access control

Access enforcement

Physical and environmental protection

Power environment and power cabling

Emergency power

System and communications protection

Security known state

System and information security

Detectable failure prevention

[Source: NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, August 2009.]

These control supplements for industrial automation and control systems are expanded as follows:

AC-3 ACCESS ENFORCEMENT

ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS.

References: NIST Special Publication 800-82.

PE-9 POWER EQUIPMENT AND POWER CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs redundant and parallel power cabling paths.

(2) The organization employs automatic voltage controls for [Assignment: organization-defined list of critical information system components].

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.

Enhancement Supplemental Guidance: Long-term alternate power supplies for the information system are either manually or automatically activated.

SC-24 FAIL IN KNOWN STATE

Control: The information system fails to an [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.

Supplemental Guidance: Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state facilitates system restart and returns to the operational mode of the organization with less disruption of mission/business processes.

SI-13 PREDICTABLE FAILURE PREVENTION

Control: The organization:

- a. Protects the information system from harm by considering mean time to failure for [Assignment: *organization-defined list of information system components*] in specific environments of operation; and
- b. Provides substitute information-system components, when needed, and a mechanism to exchange active and standby roles of the components.

Supplemental Guidance: While mean time to failure is primarily a reliability issue, this control focuses on the potential failure of specific components of the information system that provide security capability. Mean time to failure rates are defensible and based on considerations that are installation specific, not industry average. The transfer of responsibilities between active and standby information system components does not compromise safety, operational readiness, or security (e.g., state variables are preserved). The standby component is available at all times, except those in which a failure recovery is in progress or for maintenance reasons. Related control: CP-2.

Control Enhancements:

- (1) The organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than [Assignment: *organization defined fraction or percentage*] of mean time to failure.
- (2) The organization does not allow a process to execute without supervision for more than [Assignment: *organization-defined time period*].
- (3) The organization manually initiates a transfer between active and standby information system components at least once per [Assignment: *organization-defined frequency*] if the mean time to failure exceeds [Assignment: *organization-defined time period*].
- (4) The organization, if an information system component failure is detected:
 - (a) Ensures that the standby information system component successfully and transparently assumes its role within [Assignment: *organization-defined time period*]; and
 - (b) [Selection (one or more): activates [Assignment: *organization-defined alarm*]; automatically shuts down the information system].

Enhancement Supplemental Guidance: Automatic or manual transfer of roles to a standby unit may occur upon detection of a component failure.

Appendix I in NIST SP 800-53 addresses these control system supplements as well as identifies SP 800-53 controls that are candidates for tailoring to industrial automation and control systems. [Table 6-3](#) lists these candidates that have additional supplemental guidance or enhanced supplemental guidance applicable to industrial automation and control systems.

The supplemental guidance in Appendix I addressing the candidates in [Table 6-3](#) for industrial control systems is given in NIST SP 800-53 as follows:

ACCESS CONTROL

AC-2 ACCOUNT MANAGEMENT

ICS Supplemental Guidance: In situations where physical access to the ICS (e.g., workstations, hardware components, field devices) predefines account privileges or where the ICS (e.g., certain remote terminal units, meters, relays) cannot support account management, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, intrusion detection, auditing measures) in accordance with the general tailoring guidance.

Table 6-3. Security Control Tailoring Candidates for Industrial Automation and Control Systems

CONTROL NUMBER	CONTROL NAME	TAILORING OPTIONS	
		SCOPING GUIDANCE	COMPENSATING CONTROLS
AC-2	Account Management	NO	YES
AC-5	Separation of Duties	NO	YES
AC-6	Least Privilege	NO	YES
AC-7	Unsuccessful Login Attempts	NO	YES
AC-8	System Use Notification	NO	YES
AC-10	Concurrent Session Control	NO	YES
AC-11	Session Lock	NO	YES
AC-17	Remote Access	NO	YES
AC-17 (2)	Remote Access	NO	YES
AC-18 (1)	Wireless Access	NO	YES
AC-19	Access Control for Mobile Devices	NO	YES
AU-2	Auditable Events	NO	YES
AU-5	Response to Audit Processing Failure	YES	YES
AU-7	Audit Reduction and Report Generation	YES	YES
AU-12	Audit Generation	NO	YES
AU-12 (1)	Audit Generation	NO	YES
CA-2	Security Assessments	NO	YES
CP-4	Contingency Plan Testing and Exercises	NO	YES
CP-4 (1)	Contingency Plan Testing and Exercises	NO	YES
CP-4 (2)	Contingency Plan Testing and Exercises	NO	YES
CP-4 (4)	Contingency Plan Testing and Exercises	NO	YES
CP-7	Alternate Processing Site	NO	YES
IA-2	User Identification and Authentication (Organizational Users)	NO	YES
IA-3	Device Identification and Authentication	NO	YES
MA-4 (3)	Non-Local Maintenance	YES	YES
MP-5 (4)	Media Transport	YES	YES
PE-6 (2)	Monitoring Physical Access	YES	YES
RA-5	Vulnerability Scanning	NO	YES
SC-2	Application Partitioning	YES	YES
SC-3	Security Function Isolation	NO	YES
SC-7 (6)	Boundary Protection	YES	NO
SC-7 (8)	Boundary Protection	YES	YES
SC-10	Network Disconnect	NO	YES
SI-2 (1)	Flaw Remediation	YES	YES
SI-3 (1)	Malicious Code Protection	YES	YES
SI-8 (1)	Spam Protection	YES	YES

[Source: NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, August 2009.]

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support the use of automated mechanisms for the management of information system accounts, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-3 ACCESS ENFORCEMENT

ICS Supplemental Guidance: The organization ensures that access

enforcement mechanisms do not adversely impact the operational performance of the ICS.

References: NIST Special Publication 800-82.

AC-5 SEPARATION OF DUTIES

ICS Supplemental Guidance: In situations where the ICS cannot support the differentiation of roles, the organization employs appropriate compensating controls (e.g., providing increased personnel security and auditing) in accordance with the general tailoring guidance. The organization carefully considers the appropriateness of a single individual performing multiple critical roles.

AC-6 LEAST PRIVILEGE

ICS Supplemental Guidance: In situations where the ICS cannot support differentiation of privileges, the organization employs appropriate compensating controls (e.g., providing increased personnel security and auditing) in accordance with the general tailoring guidance. The organization carefully considers the appropriateness of a single individual having multiple critical privileges.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

ICS Supplemental Guidance: In situations where the ICS cannot support account/node locking or delayed login attempts, or the ICS cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., logging or recording all unsuccessful login attempts and alerting ICS security personnel through alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded) in accordance with the general tailoring guidance.

AC-8 SYSTEM USE NOTIFICATION

ICS Supplemental Guidance: In situations where the ICS cannot support system use notification, the organization employs appropriate compensating controls (e.g., posting physical notices in ICS facilities) in accordance with the general tailoring guidance.

AC-10 CONCURRENT SESSION CONTROL

ICS Supplemental Guidance: In situations where the ICS cannot support concurrent session control, the organization employs appropriate compensating controls (e.g., providing increased auditing measures) in accordance with the general tailoring guidance.

AC-11 SESSION LOCK

ICS Supplemental Guidance: The ICS employs session lock to prevent access to specified workstations/nodes. The ICS activates session lock mechanisms automatically after an organization-defined time period for designated workstations/nodes on the ICS. In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Session lock is not a substitute for logging out of the ICS. In situations where the ICS cannot support session lock, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

AC-17 REMOTE ACCESS

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of remote access methods, the organization employs nonautomated mechanisms or procedures as compensating controls (e.g., following manual authentication [see IA-2 in this appendix], dial-in remote access may be enabled for a specified period of time, or a call may be placed from the ICS site to the authenticated remote entity) in accordance with the general tailoring guidance.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For

example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The organization explores all possible cryptographic mechanisms (e.g., encryption, digital signature, hash function). Each mechanism has a different delay impact. In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on safety, performance, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing for remote sessions or limiting remote access privileges to key personnel) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

AC-18 WIRELESS ACCESS

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity, and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The organization explores all possible cryptographic mechanisms (e.g., encryption, digital signature, hash function). Each mechanism has a different delay impact. In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of wireless access, or the components cannot use cryptographic mechanisms due to significant adverse impact on safety, performance, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing for wireless access or limiting wireless access privileges to key personnel) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other

mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-22 PUBLICLY ACCESSIBLE CONTENT

ICS Supplemental Guidance: Generally, public access to ICS information is not permitted.

AWARENESS AND TRAINING

AT-2 SECURITY AWARENESS

ICS Supplemental Guidance: Security awareness training includes initial and periodic review of ICS specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security awareness program is consistent with the requirements of the security awareness and training policy established by the organization.

AT-3 SECURITY TRAINING

ICS Supplemental Guidance: Security training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security training program is consistent with the requirements of the security awareness and training policy established by the organization.

AUDITING AND ACCOUNTABILITY

AU-2 AUDITABLE EVENTS

ICS Supplemental Guidance: Most ICS auditing occurs at the application level.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

ICS Supplemental Guidance: In general, audit record processing is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing, including response to audit failures, the organization employs compensating controls (e.g., providing a *Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations* auditing capability on a separate information system) in accordance with the general tailoring guidance.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

ICS Supplemental Guidance: In general, audit reduction and report generation is not performed on the ICS but on a separate information system. In situations where the ICS cannot support auditing, including audit reduction and report generation, the organization employs compensating controls (e.g., providing an auditing capability on a separate information system) in accordance with the general tailoring guidance.

AU-12 AUDIT GENERATION

ICS Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

SECURITY ASSESSMENT AND AUTHORIZATION

CA-2 SECURITY ASSESSMENTS

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (i.e., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before an assessment can be conducted. If an ICS must be taken offline to conduct an assessment, the assessment is scheduled to occur during planned ICS outages whenever possible. In situations where the organization cannot, for operational reasons, conduct a live assessment of a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct the assessment) in accordance with the general tailoring guidance.

CA-7 CONTINUOUS MONITORING

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (i.e., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. Ongoing assessments of ICS may not be feasible. See CA-2 ICS Supplemental Guidance in this appendix.

CONFIGURATION MANAGEMENT

CM-3 CONFIGURATION CHANGE CONTROL

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to implement configuration change control, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-4 SECURITY IMPACT ANALYSIS

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to enforce access restrictions and support auditing of enforcement actions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (3)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot prevent the installation of software programs that are not signed with an organizationally recognized and approved certificate, the organization employs alternative mechanisms or procedures as compensating controls (e.g., auditing of software installation) in accordance with the general tailoring

guidance.

CM-6 CONFIGURATION SETTINGS

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-7 LEAST FUNCTIONALITY

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot employ automated mechanisms to prevent program execution, the organization employs compensating controls (e.g., external automated mechanisms, procedures) in accordance with the general tailoring guidance.

CONTINGENCY PLANNING

CP-2 CONTINGENCY PLAN

ICS Supplemental Guidance: The organization defines contingency plans for categories of disruptions or failures. In the event of a loss of processing within the ICS or communication with operational facilities, the ICS executes predetermined procedures (e.g., alert the operator of the failure and then do nothing, alert the operator and then safely shut down the industrial process, alert the operator and then maintain the last operational setting prior to failure).

Consideration is given to restoring system state variables as part of restoration (e.g., valves are restored to their original settings prior to the disruption).

References: NIST Special Publication 800-82.

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

ICS Supplemental Guidance: In situations where the organization cannot test

or exercise the contingency plan on production ICS due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., using scheduled and unscheduled system maintenance activities, including responding to ICS component and system failures, as an opportunity to test or exercise the contingency plan) in accordance with the general tailoring guidance.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

ICS Supplemental Guidance: Reconstitution of the ICS includes restoration of system state variables (e.g., valves are restored to their appropriate settings as part of the reconstitution).

IDENTIFICATION AND AUTHENTICATION

IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is critical. Local emergency actions for ICS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. In situations where the ICS cannot support user identification and authentication, or the organization determines it is not advisable to perform user identification and authentication due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance. For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access.

See AC-17 ICS Supplemental Guidance in this appendix. Local user access to ICS components is enabled only when necessary, approved, and authenticated.

Control Enhancements: (1) (2) (3)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support multifactor authentication, the organization employs compensating controls in accordance with the general tailoring guidance (e.g., implementing physical security measures).

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

ICS Supplemental Guidance: In situations where the ICS cannot support device identification and authentication (e.g., serial devices), the organization employs compensating controls (e.g., implementing physical security measures) in accordance with the general tailoring guidance.

IA-4 IDENTIFIER MANAGEMENT

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification may be role-based, group-based, or device-based.

References: NIST Special Publication 800-82.

IA-5 AUTHENTICATOR MANAGEMENT

References: NIST Special Publication 800-82.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

ICS Supplemental Guidance: The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

INCIDENT RESPONSE

IR-6 INCIDENT REPORTING

ICS Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) maintains the ICS Security Center at http://www.uscert.gov/control_systems.

References: NIST Special Publication 800-82.

MAINTENANCE

MA-4 NONLOCAL MAINTENANCE

Control Enhancement: (3)

ICS Enhancement Supplemental Guidance: In crisis or emergency situations, the organization may need immediate access to nonlocal maintenance and diagnostic services in order to restore essential ICS operations or services. In situations where the organization may not have access to nonlocal maintenance or diagnostic service at the required level of security, the organization employs appropriate compensating controls (e.g., limiting the extent of the maintenance and diagnostic services to the minimum essential activities, carefully monitoring and auditing the nonlocal maintenance and diagnostic activities) in accordance with the general tailoring guidance.

MEDIA PROTECTION

MP-5 MEDIA TRANSPORT

Control Enhancement: (4)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support cryptographic mechanisms, the organization employs compensating controls in accordance with the general tailoring guidance (e.g., implementing physical security measures).

PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-3 PHYSICAL ACCESS CONTROL

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event, the organization may restrict access to ICS facilities and assets to authorized individuals only. ICS are often constructed of devices that either do not have or cannot use comprehensive access control capabilities due to time-restrictive safety constraints. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to fulfill the security requirements of the organization's security plan.

References: NIST Special Publication 800-82.

PLANNING

PL-2 SYSTEM SECURITY PLAN

References: NIST Special Publication 800-82.

RISK ASSESSMENT

RA-2 SECURITY CATEGORIZATION

References: NIST Special Publication 800-82.

RA-3 RISK ASSESSMENT

References: NIST Special Publication 800-82.

RA-5 VULNERABILITY SCANNING

ICS Supplemental Guidance: Vulnerability scanning and penetration testing are used with care on ICS networks to ensure that ICS functions are not adversely impacted by the scanning process. Production ICS may need to be taken off-line, or replicated to the extent feasible, before scanning can be conducted. If ICS are taken off-line for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. In situations where the organization cannot, for operational reasons, conduct vulnerability scanning on a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct scanning) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

SYSTEM AND SERVICES ACQUISITION

SA-4 ACQUISITIONS

ICS Supplemental Guidance: The SCADA/Control Systems Procurement Project provides example cybersecurity procurement language for ICS.

References: Web: www.msisc.org/scada.

SA-8 SECURITY ENGINEERING PRINCIPLES

References: NIST Special Publication 800-82.

SYSTEM AND COMMUNICATIONS PROTECTION

SC-2 APPLICATION PARTITIONING

ICS Supplemental Guidance: In situations where the ICS cannot separate user functionality from information system management functionality, the organization employs compensating controls (e.g., providing increased auditing measures) in accordance with the general tailoring guidance.

SC-3 SECURITY FUNCTION ISOLATION

ICS Supplemental Guidance: In situations where the ICS cannot support security function isolation, the organization employs compensating controls (e.g., providing increased auditing measures, limiting network connectivity) in accordance with the general tailoring guidance.

SC-7 BOUNDARY PROTECTION

Control Enhancements: (1) (2)

ICS Enhancement Supplemental Guidance: Generally, public access to ICS information is not permitted.

Control Enhancement: (6)

ICS Enhancement Supplemental Guidance: The organization selects an appropriate failure mode (e.g., fail closed, fail open).

SC-8 TRANSMISSION INTEGRITY

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The organization explores all possible cryptographic integrity mechanisms (e.g., digital signature, hash function). Each mechanism has a different delay impact.

SC-9 TRANSMISSION CONFIDENTIALITY

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-10 NETWORK DISCONNECT

ICS Supplemental Guidance: In situations where the ICS cannot terminate a network connection at the end of a session or after an organization-defined time period of inactivity, or the ICS cannot terminate a network connection due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing measures or limiting remote access privileges to key personnel) in accordance with the general tailoring guidance.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

ICS Supplemental Guidance: The use of cryptography, including key management, is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The use of cryptographic key management in ICS is intended to support internal nonpublic use.

SC-13 USE OF CRYPTOGRAPHY

ICS Supplemental Guidance: The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-14 PUBLIC ACCESS PROTECTIONS

ICS Supplemental Guidance: Generally, public access to ICS is not permitted.

SC-15 COLLABORATIVE COMPUTING DEVICES

ICS Supplemental Guidance: Generally, collaborative computing mechanisms are not permitted on ICS.

SC-19 VOICE OVER INTERNET PROTOCOL

ICS Supplemental Guidance: The use of VoIP technologies is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-23 SESSION AUTHENTICITY

ICS Supplemental Guidance: In situations where the ICS cannot protect the authenticity of communications sessions, the organization employs compensating controls (e.g., auditing measures) in accordance with the general tailoring guidance.

SYSTEM AND INFORMATION INTEGRITY

SI-2 FLAW REMEDIATION

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage flaw remediation and automatic updates, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to conduct and report on the status of flaw remediation, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

SI-3 MALICIOUS CODE PROTECTION

ICS Supplemental Guidance: The use of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage malicious code protection mechanisms, the organization employs appropriate compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to update malicious code protection mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

SI-4 INFORMATION SYSTEM MONITORING

ICS Supplemental Guidance: The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the ICS.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated tools to support near-real-time analysis of events, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (6)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot prevent nonprivileged users from circumventing intrusion detection and prevention capabilities, the organization employs appropriate compensating controls (e.g., enhanced auditing) in accordance with the general tailoring guidance.

SI-6 SECURITY FUNCTIONALITY VERIFICATION

ICS Supplemental Guidance: Generally, it is not recommended to shut down and restart the ICS upon the identification of an anomaly.

SI-7 SOFTWARE AND INFORMATION INTEGRITY

ICS Supplemental Guidance: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ICS.

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ICS.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot employ automated tools that provide notification of integrity discrepancies, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general

tailoring guidance.

SI-8 SPAM PROTECTION

ICS Supplemental Guidance: The organization removes unused and unnecessary functions and services (e.g., electronic mail, Internet access). Due to differing operational characteristics between ICS and general purpose information systems, ICS do not generally employ spam protection mechanisms. Unusual traffic flow (e.g., during crisis situations), may be misinterpreted and detected as spam, which can cause issues with the ICS and possible system failure.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage spam protection mechanisms, the organization employs local mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Department of Homeland Security, Catalog of Control Systems Security: Recommendations for Standards Developers

The Department of Homeland Security (DHS) catalog⁶ is based on NIST SP 800-53 and is described in the document as presenting “a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyberattacks.” The controls in the catalog are divided into 19 categories or families that are taken primarily from NIST SP 800-53, Revision 3, with some controls from ANSI/ISA-99.00.02⁷. There are 250 controls in the DHS control systems security catalog as opposed to 347 in NIST SP 800-53.

The control families from the catalog and their relationship to NIST SP 800-53 categories are shown in [Table 6-4](#).

AMI System Security Requirements

Security requirements for the Advanced Metering Infrastructure (AMI) have been developed by the AMI Security (AMI-SEC) Task Force under the title of *AMI System Security Requirements*⁸. The purpose of these requirements, as stated in the Task Force document, is:

Table 6-4. DHS Security Controls Catalog and Relationship to NIST SP 800-53

NIST SP 800-53A Revision 3 Families	
2a Security Policy	Control family initial elements relates to its own policy and procedures (e.g., AC- 1 through PM-1)
2b Organizational Security	Program Management—PM
2c Personnel Security	Personnel Security—PS
2d Physical and Environmental Security	Physical and Environmental Security—PE
3 System and Service Acquisition	System and Service Acquisition—SA
2c Configuration Management	Configuration Management—CM
2b Planning	Planning—PP
2c System and Communication Protection	System and Communication Protection—SC
2c Information and Content Management	Information and Content Management—IP
2b Media Protection	Media Protection—MP
2b System Development and Maintenance	System Development and Maintenance—SD
2b Awareness and Training	Awareness and Training—AT
2b Incident Response	Incident Response—IR
2b Media Protection	Media Protection—MP
3 System and Information Integrity	System and Information Integrity—SI
2c Access Control	Access Control—AC
2c Identification Authentication	Identification Authentication—IA
2c Audit and Accountability	Audit and Accountability—AU
2c System Security Policy	System Security Policy—SP
2c Risk Management	Risk Management—RM
2c Security Management	Security Management—SM

[Source: Department of Homeland Security, *Catalog of Control Systems Security: Recommendations for Standards Developers*, April 2011.]

To provide the utility industry along with supporting vendor communities and other stakeholders a set of security requirements that should be applied to AMI implementations to ensure the high level of information assurance, availability, and security necessary to maintain a reliable system and consumer confidence. While this specification focuses on AMI, the security requirements contained in the document may be extended to other network-centric, Smart Grid solutions.

The AMI security requirements are characterized by letters as follows:

- “F” are functional requirements.
- “S” are supporting services to functional requirements.
- “A” are assurance requirements.
- Remaining letters in the identifier help associate the requirement with its requirement class.

Table 6-5 summarizes the AMI system security control requirements.

Table 6-5. AMI System Security Controls

	Description
Confidentiality and Privacy (FCP)	service, or object protection, against discovery and misuse of identity by other users/subjects.
Integrity (FIN)	Integrity increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner.
Availability (FAM)	addresses the ability of the system to continue to operate and satisfy business/mission needs under diverse operating conditions, including but not limited to peak load conditions, attacks, maintenance operations, and normal operating conditions.
Identification (FID)	controls associated with who an actor claims to be.
Authentication (FAT)	requirements around the proof of identity of an actor.
Authorization (FAZ)	overs the approval of an actor to perform an action.
Non-repudiation (FNR)	Address the ability to tie an actor to an action.
Accounting (FAC)	Requires the recording of activity by actors/elements throughout the system and providing the means to perform a successful audit of events that occur on the system.
Threat Detection Services (FES)	Services applied to detect events outside of the bounds of normally anticipated or desired behavior, such as attacks, intrusions, or errors.
Boundary Services (FBS)	Requirements for boundary services that provide isolation between system elements or between the system and external entities.
Cryptographic Services (FCB)	cryptographic services, which include encryption, signing, key management and key revocation with the security objectives of identification and authentication, nonrepudiation, trusted path, trusted channel and data separation.
Notification and Signaling Services (FNS)	and signaling services, which are oriented towards providing system activity information and command result logging.
Resource Management Services (FRS)	management services requirements, including management of runtime resources such as network/communication paths, processors, memory or disk space (e.g., for audit log capacity), and other limited system resources.
Trust and Certificate Services (FTC)	Definition of relationships between entities and the faith placed on the relationship certificates that have uses outside of cryptography; for example, material relating to creation, storage, and revocation of certificates.
Development Rights (ADR)	AMI System Security Specification requirements regarding the activities involved in developing Smart Grid system solutions. Topics include acquisition issues, configuration management and development practices.
Organizational Rights (AOR)	Requirements regarding the policies employed by the organization(s) with access to assets of a deployed Smart Grid system. These requirements reflect on an organization's ability to continue to operate a Smart Grid system reliably over time. Topics include training procedures, personnel security, strategic planning, and monitoring and reviewing security policies.
Fielding/Operating Rights (AOF)	Requirements regarding the activities involved in the day-to-day operation of deployed Smart Grid systems. Topics include information and document management policies, incident response procedures, maintenance procedures, physical and environmental security, and media protection.

~~The controls in the A&E~~ requirements are based on security auditing and recognizing, recording, storing, and analyzing information related to security relevant activities. The resulting audit records can be examined to determine which security relevant activities took place and who (which user) is responsible for them.

~~The controls in the A&E~~ section is ensuring that resources are only accessed by the appropriate personnel and that personnel are correctly identified. Mechanisms also need to be put into place to monitor access activities for inappropriate activity.

[Source: Advanced Metering Infrastructure Security Task Force (AMI-SEC), *AMI System Security Requirements*, V1.01, 12/17/2008.]

The format of a typical AMI security function is as follows:

Identification (FID)

This section covers requirements around who a user claims to be.

FID.1 The security function shall require each user to be successfully identified before allowing any other system's security function-mediated actions on behalf of that user unless it is one of the following: [*list of system's security function-mediated actions*] that may be allowed before the user is identified.

FID.2 The security function shall associate the following user security attributes with subjects acting on behalf of that user: [*Assignment: list of user security attributes*].

FID.3 The security function shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users: [*Assignment: rules for the initial association of attributes*].

FID.4 The security function shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*Assignment: rules for the changing of attributes*].

FID.5 The security function shall uniquely identify (and authenticate) [*Assignment: users, processes acting on behalf of users, devices, etc.*] before establishing a connection.

FID.6 The organization shall manage user identifiers by:

- 1.Uniquely identifying each user
- 2.Verifying the identity of each user

- 3.Receiving authorization to issue a user identifier from an appropriate organization official
- 4.Issuing the user identifier to the intended party
- 5.Disabling the user identifier after [Assignment: organization-defined time period] of inactivity
- 6.Archiving user identifiers.

FID.7 The security function shall have mechanisms to uniquely identify (and authenticate) [Assignment: users, processes acting on behalf of users, etc.].

FID.8 The security function shall appropriately label information in storage, in process, and in transmission.

Department of Defense Instruction Number 8500.2, *Information Assurance (IA) Implementation*

Department of Defense Instruction Number 8500.2²⁹ puts forth a baseline level of information assurance (IA) controls for information systems. A large number of these controls can be adapted and applied to industrial control and automation systems by taking into account the similarities and differences between IT and automation and control systems. The controls are divided into eight groups and, as stated in Instruction 8500.2, each control “describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities.” The objective condition is testable, compliance is measurable, and the activities required to achieve the IA control are assignable and thus accountable.

Table 6-6 lists the eight Instruction 8500.2 control subject areas.

Table 6-6. DoD Instruction 8500.2 Control Subject Areas

Number	Subject area
DC	Security design and configuration
IA	Identification and authentication
EC	Enclave and computing environment
EB	Enclave boundary defense
EE	Physical and environmental
PR	Personnel
CO	Continuity
VI	Vulnerability and incident management

[Source: Department of Defense Instruction Number 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003.]

Examples of the format of Instruction 8500.2 controls from each of the eight subject areas are as follows:

Security Design and Configuration Integrity
DCPA-1 Partitioning the Application

User interface services (e.g., Web services) are physically or logically separated from data storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, combinations of these methods, or other methods, as appropriate.

Identification and Authentication Integrity
IAKM-2 Key Management

Symmetric Keys are produced, controlled and distributed using NSA-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

Enclave and Computing Environment Integrity
ECND-2 Network Device Controls

An effective network device control program (e.g., routers, switches, firewalls) is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA). Audit or other technical measures are in place to ensure that the network device controls are not compromised. Change controls are periodically tested.

Enclave Boundary Defense Availability
EBVC-1 VPN Controls

All VPN traffic is visible to network intrusion detection systems (IDS).

Physical and Environmental Availability
PETC-2 Temperature Controls

Automatic temperature controls are installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.

Personnel Availability

PRRB-1 Security Rules of Behavior or Acceptable Use Policy

A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.

Continuity Availability

CODP-2 Disaster and Recovery Planning

A disaster plan exists that provides for the resumption of mission or business essential functions within 24 hours of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

Vulnerability and Incident Management Availability

VIVM-1 Vulnerability Management

A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted.

Consolidation of Best Practices Controls for Industrial Automation and Control Systems

The preceding sections presented some of the most effective controls that can be applied to automation and control systems and provide excellent guidance for securing these systems. A consolidation of the best practices from all the reviewed controls would be useful to the practitioners and management in the industrial control and automation field for use in everyday applications.

[Table 6-7](#) provides this information with references to the source documents to provide a solid basis for the justification and origin of these controls. This table is intended to provide a quick, useful reference to implementing the best security practices for the control engineer, technician, supervisor, and management of the key elements of manufacturing operations, process plants, and the critical infrastructure.

Table 6-7. Controls Summary Table and Source References

Control #	Industrial automation and control system security control	Comments	Source
1.	Implement Access Control	Implement processes for arbitrating requests for access to critical system information.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
2.	Conduct Risk Assessment	Identify risks to systems including potential impacts, probabilities, and mitigation options.	SP 800-82, SP 800-53, DHS catalog, AMI, 8500.2
3.	Remove Default Accounts	Many automation system manufacturers have default accounts and passwords in place for maintenance or system access. These accounts should be deleted and any default passwords changed or eliminated.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
4.	Develop Security Policies	Have policies in place that express management intent, address the security mission, define roles and responsibilities, and address the use of computational resources.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
5.	Develop Security Plan	Generate a plan to define and implement security controls, conduct incident response and evaluate security throughout the system's life cycle.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
6.	Develop Personnel Screening Policies and Procedures	Implement personnel-related policies and procedures, including screening, transfers, and termination.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
7.	Manage Maintenance	Develop and implement policies and procedures to address all parts of system maintenance.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
8.	Protect System Information Integrity	Implement policies and procedures to ensure the integrity of data.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
9.	Develop Hiring Policies	Implement policies for employee background checks, employment terms, responsibilities, and so on.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2

10.	Develop Acquisition Policies	Apply risk-assessment-based acquisition policies throughout the system's life cycle.	SP 800-82, SP 800-53, DHS catalog, AMI, 8500.2
11.	Provide for Strong Authentication	Employ strong authentication mechanisms at interfaces to the Internet and any other public networks.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
12.	Test and evaluate critical software	Implement mechanisms to evaluate software elements for vulnerabilities.	SP 800-82, TR99.00.01, DHS catalog, AMI, 8500.2
13.	Implement Audit Procedures	Provide for independent evaluation of audit records to determine adequacy of security controls and compliance.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
14.	Implement an Effective Password Policy	Establish a strong password policy that specifies characteristics, such as length, types of characters, audit frequency, and change periods. The password policy should take into account the balance required between the types of password protected access mechanisms used and the need for an automation system operator to quickly access system components under stress in the event of an emergency.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
15.	Identify Critical System Elements	Determine the critical system elements that have to be protected and included in disaster recovery planning.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
16.	Apply Defense in Depth	Apply security in layers, beginning with perimeter defense and employing SCADA-aware firewalls and intrusion detection and prevention systems.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, 8500.2
17.	Protect Critical Data and Media	Protect sensitive information in all stages of its life cycle, include its use, storage, transit, and disposal. Encryption should be applied according to good security principles.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2

18.	Provide for Physical Security	Implement physical security controls including back-up power, fire detection and prevention, physical access controls, cameras, badges, and tokens.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
19.	Develop an Up-to-Date System Diagram	Prepare and maintain a diagram of the automation system, including topologies, devices (such as PLCs), software in use, protection mechanisms, locations of devices, transducers, and sensors.	SP 800-82, SP 800-53, DHS catalog, AMI, 8500.2
20.	Protect Equipment	When possible, place equipment in locations that prevent unauthorized access.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
21.	Develop and Implement a Patching Policy	When compatible with real-time and production requirements, test and install patches to critical software that address vulnerabilities. Patches should not be installed on production systems without evaluation on test systems or off-line to ensure that no faults are introduced into production equipment.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, 8500.2
22.	Conduct Vulnerability Assessments	When compatible with real-time and production requirements, perform vulnerability assessments in a manner that does not interfere with system operation.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
23.	Implement System Logging	Log and review critical system parameters in a manner compatible with the production requirements of automation and control systems.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
24.	Manage and Control Remote Access	It is important to control and manage remote access using strong authentication and encrypted links, such as VPNs. Give special security consideration to wireless devices and desktop modems.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
25.	Protect communications	Implement methods to protect system transmission elements.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2

26.	Implement filtering and screening	Use devices such as firewalls to protect critical data and support access control.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
27.	Provide Security Awareness Training	Provide personnel with security awareness training to alert them to issues such as social engineering, and phishing. They should also be informed on how to determine if an incident has occurred, whom to notify if an incident has occurred, and any actions to be taken in that event.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
28.	Maintain Only Necessary Services	Disable any unnecessary systems services and unused open ports.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, 8500.2
29.	Undergo Certification and Accreditation	Obtain certification and accreditation and accept residual risk.	SP 800-82, SP 800-53, DHS catalog, AMI (accreditation)
30.	Employ Configuration Management	Implement configuration management practices that document any system hardware and software changes.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
31.	Implement Back-Ups	Arrange for backing up system hardware, software, and data in the event of a disaster or other failure of critical systems.	SP 800-82, TR99.00.01, DHS catalog, AMI, 8500.2
32.	Develop Business Continuity and Disaster Recovery Plans	Develop, test, and implement disaster recovery and business continuity plans.	NIST 800-82, SP 800-53, DHS catalog, AMI, 8500.2
33.	Secure Extranets	Minimize and secure partner networks or extranets if they are necessary.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2
34.	Use Antivirus Software Intelligently	Implement antivirus software, taking into account the limitations and requirements of automation systems, including its effect on response time and memory capacity.	SP 800-82, TR99.00.01, SP 800-53, DHS catalog, AMI, 8500.2

35.	Implement Program Management	The program management plan specifies the individuals within the organization responsible for the security program management controls and the appointment of a senior information security officer, ensures that all capital planning and investment requests include the resources needed to implement the information security program, develops an enterprise architecture with consideration for information security, and defines mission/ business processes with consideration for information security and the resulting risk to the organization, personnel, and the critical infrastructure.	SP 800-53, DHS catalog, AMI
36.	Predictable Failure Prevention	Control that protects the information system from harm by considering mean time to failure for critical components in specific environments of operation.	SP 800-53, DHS catalog, AMI

Summary

Chapter 6 presents the most popular and effective controls designed to secure industrial automation and control systems specifically or which could be adapted to such systems. These standards and guidelines form a comprehensive, structured methodology for protecting manufacturing facilities, process plants, and the critical infrastructure. A useful output of this chapter is the consolidation of these best practices to provide a single reference source as a baseline for securing industrial automation and control systems.

Review Questions for Chapter 6

1. NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, partitions security controls into which one of the following groups?
 - a. Management controls, operational controls, and technical controls
 - b. Management controls, administrative controls, and technical controls
 - c. Management controls, operational controls, and physical controls

d.Logical controls, operational controls, and technical controls

2.NIST SP 800-82 defines five major security objectives for an industrial control system (ICS) implementation. Which of the following is NOT one of those objectives?

- a.Restricting logical access to the ICS network and network activity
- b.Restricting physical access to the ICS network and devices
- c.Protecting individual ICS components from exploitation
- d.Shutting down the ICS after an incident

3.In NIST SP 800-82, policies and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation is known as which of the following?

- a.Configuration management
- b.Risk management
- c.System management
- d.System maintenance

4.In the NIST SP 800-82 controls, the process of granting or denying specific requests for obtaining and using information and related information processing services for physical access to areas within the information system environment is known as which of the following?

- a.Authentication
- b.Audit and accountability
- c.Access control
- d.Identification

5.The controls of ANSI/ISA-TR99.00.01-2007 are organized into six categories. Which of the following is NOT one of those categories?

- a.Encryption Technologies and Data Validation
- b.Risk Mitigation Technologies
- c.Authentication and Authorization Technologies

d.Filtering/Blocking/Access Control Technologies

6.ANSI/ISA-TR99.00.01-2007 describes which of the following as “the initial step in protecting an industrial automation and control system (IACS) and its critical assets from unwanted breaches. It is the process of determining who and what should be allowed into or out of a system”?

- a.Authorization
- b.Authentication
- c.Identification
- d.Confirmation

7.Which of the following are the major components of authentication and authorization technologies spelled out in ANSI/ISA-TR99.00.01-2007?

- a.Role-based, password, and challenge response
- b.Rule-based, user ID, and challenge response
- c.Role-based, password, and call-back
- d.Rule-based, password, and call-back

8.Which of the following does ANSI/ISA-TR99.00.01-2007 identify as the three main types of software that have to be considered in industrial automation and control system software?

- a.Mobile operating systems, real-time and embedded operating systems, and Web servers and Internet technologies
- b.Server and workstation operating systems, real-time and embedded operating systems, and wireless technologies
- c.Server and workstation operating systems, real-time and embedded operating systems, and Web servers and Internet technologies
- d.Server and workstation operating systems, real-time and embedded operating systems, and mobile technologies

9.In ANSI/ISA-TR99.00.01-2007, what are the three main categories of physical security elements?

- a.Active, identification and monitoring devices, and passive
- b.Active, real-time, and passive

- c.Active, identification and monitoring devices, and real-time
- d.Reactive, identification and monitoring devices, and passive

10.The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cybersecurity Standards are divided into Standards CIP-002-4 through CIP-009-4 and address “the identification and protection of critical cyber assets to support reliable operation of the Bulk Electric System (BES).” Which of the following is NOT one of the eight standards?

- a.Risk assessment
- b.Critical cyber asset identification
- c.Security management controls
- d.Electronic security perimeters

11.Which NERC CIP standard “ensures the identification, classification, response, and reporting of cybersecurity incidents related to critical cyber assets?”

- a.Physical security of critical cyber assets
- b.Systems security management
- c.Recovery plans for critical cyber assets
- d.Incident reporting and response planning

12.In NIST SP 800-53, the security controls are divided into 17 families, each with a unique, two-character identifier. The control families are themselves partitioned into three classes. Which of the three classes does the control family titled CP (contingency planning) fall under?

- a.Technical
- b.Management
- c.Operational
- d.Administrative

13.The NIST SP 800-53 controls are considered baseline controls, which can be tailored to more closely meet the needs of a particular organization and automation system. Which of the following is NOT one of the elements of the NIST SP 800-53 tailoring process?

- a.Selecting (or specifying) compensating security controls, if

needed, to adjust the preliminary set of controls to obtain an equivalent set deemed to be more feasible to implement

- b. Applying scoping guidance to the initial baseline security controls to obtain a preliminary set of applicable controls for the tailored baseline
- c. Specifying organization-defined parameters in the security controls via explicit assignment and selection statements to complete the definition of the tailored baseline
- d. Developing custom parameters to meet the needs of the control system

14. The NIST SP 800-53 tailoring process refers to guidance “designed to ensure that only the controls appropriate to the particular mission and requirements of the organization are used.” This guidance is referred to as which of the following?

- a. Correlating
- b. Assessing
- c. Evaluating
- d. Scoping

15. NIST SP 800-53 provides for the use of security controls, which the publication defines as “a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control ... that provides an equivalent or comparable level of protection for an information system and the information processed, stored, or transmitted by that system.” This type of additional control is known as which of the following?

- a. Supporting
- b. Supplemental
- c. Compensating
- d. Custom

16. Recognizing some of the special requirements of industrial automation and control systems, NIST SP 800-53 defines supplements to the baseline control systems to address automation and control issues. Which one of the following is NOT one of these supplements?

- a. Risk evaluation

- b. Predictable failure prevention
- c. Emergency power
- d. Access enforcement

17. The Department of Homeland Security's *Catalog of Control Systems Security* is based on which of the following security controls documents?

- a. NIST SP 800-82
- b. NIST SP 800-53
- c. NIST SP 800-39
- d. The NERC CIP Cybersecurity Standards

18. The Advanced Metering Infrastructure (AMI) Security Requirements are characterized by letters. Which of the following is NOT one of the AMI security requirements categories?

- a. "R" are risk requirements
- b. "F" are functional requirements
- c. "S" are supporting services to functional requirements
- d. "A" are assurance requirements

19. The AMI security requirement FIN refers to which of the following security principles?

- a. Inventory
- b. Final evaluation
- c. Integrity
- d. Internal

20. The recording of activity by actors/elements throughout the system and providing the means to perform a successful audit of events that occur on the system refers to which of the following AMI security controls?

- a. Accounting
- b. Anomaly detection
- c. Authentication
- d. Authorization

21. Which of the following is NOT one of the Department of Defense Instruction 8500.2 security control subject areas?
- a. Security design and configuration
 - b. Risk management
 - c. Physical and environmental
 - d. Continuity
22. Department of Defense Instruction 8500.2, control CODP, Disaster and Recovery Planning, provides which of the following information security principles?
- a. Availability
 - b. Integrity
 - c. Accountability
 - d. Authentication
23. In NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, risk assessment, planning, systems and services acquisition, certification, accreditation, and security assessments fall under what category of controls?
- a. Technical
 - b. Logical
 - c. Management
 - d. Operational
24. In NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, controls such as personnel security and contingency planning fall under which of the following control categories?
- a. Management
 - b. Operational
 - c. Technical
 - d. Physical
25. In NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, controls, such as identification and authentication, access control, and audit and accountability fall under which of the following control categories?

- a.Administrative
- b.Operational
- c.Management
- d.Technical

26.ANSI/ISA-TR99.00.01-2007, *Security Technologies for Industrial Automation and Control Systems*, defines which of the following principles as “the process of positively identifying potential network users, hosts, applications, services, and resources, using a combination of identification factors or credentials. The result of this process then becomes the basis for permitting or denying further actions”?

- a.Authentication
- b.Authorization
- c.Accountability
- d.Accessibility

27.ANSI/ISA-TR99.00.01-2007, *Security Technologies for Industrial Automation and Control Systems*, divides authentication into which of the following two areas?

- a.User authentication and group authentication
- b.Group authentication and network service authentication
- c.User authentication and network service authentication
- d.Platform authentication and user authentication

28.ANSI/ISA-TR99.00.01-2007 defines which of the following as “can be used to distinguish communication by devices that are not part of the desired network. This feature is generally attractive for SCADA and other process control systems that wish to allow little or no access to the control network, but is difficult to deploy in systems requiring unrestricted Internet access”?

- a.Asymmetric key encryption
- b.Digital signature
- c.Biometrics
- d.Symmetric key encryption

29.ANSI/ISA-TR99.00.01-2007 states that encryption can also be employed in a virtual private network (VPN), which provides for authentication,

integrity, and protection from unauthorized disclosure. Which of the following is NOT one of the most common VPN implementations?

- a.Hyper Text Transfer Protocol (HTTP)
- b.Internet Protocol Security (IPSec)
- c.Secure Shell (SSH)
- d.Secure Sockets Layer (SSL)

30.What standards address “the identification and protection of critical cyber assets to support reliable operation of the Bulk Electric System (BES)?”

- a.ANSI/ISA-TR99.00.01-2007
- b.NIST SP 800-53
- c.NIST SP 800-82
- d.NERC CIP Cybersecurity Standards

31.Which of the following is NOT one of the NERC CIP Cybersecurity Standards?

- a.Risk Management
- b.Critical Cyber Asset Identification
- c.Security Management Controls
- d.Personnel and Training

32.The following are characterized as what type of guidance in NIST SP 800-53: determining the primary security objectives, which system components the controls are applicable to, and what technologies are employed in the system?

- a.Custom
- b.Complementary
- c.Scoping
- d.Supplemental

33.In NIST SP 800-53, one of the industrial control system supplemental controls states that “it protects the information system from harm by considering mean time to failure for [*Assignment: organization-defined list of information system components*] in specific environments of operation.” This industrial control system industrial supplemental control is which of the following?

- a. Predictable Failure Prevention
- b. Fail in a Known State
- c. Access Enforcement
- d. Emergency Power

34. The Organizational Security controls in the Department of Homeland Security *Catalog of Control Systems Security* relate to which of the following control categories in NIST SP 800-53?

- a. Personnel Security (PS)
- b. System and Services Acquisition (SA)
- c. Access Control (AC) and Program Management (PM)
- d. Contingency Planning (CP) and Media Protection (MP)

35. The Monitoring and Reviewing Control System Security Policy controls in the *Catalog of Control Systems Security* relate to which of the following control categories in NIST SP 800-53?

- a. Audit and Accountability (AU)
- b. Program Management (PM)
- c. Security Assessment and Authorization (CA)
- d. System and Information Integrity (SI)

36. The AMI System Security Requirement that addresses “the proof of identity of an actor” is which of the following?

- a. Authentication
- b. Identification
- c. Authorization
- d. Nonrepudiation

37. The AMI System Security Requirement that is “based on security auditing and recognizing, recording, storing, and analyzing information related to security relevant activities” is which of the following?

- a. Authorization
- b. Authentication
- c. Accountability

References

- 1 NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, September 2008.
- 2 NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009.
- 3 ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*, October 2007.
- 4 North American Electric Reliability Corporation (NERC), *Critical Infrastructure Protection (CIP) Cybersecurity Standards*, 2011.
- 5 NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009.
- 6 Department of Homeland Security, *Catalog of Control Systems Security: Recommendations for Standards Developers*, April 2011.
- 7 ANSI/ISA-99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, 2009.
- 8 Advanced Metering Infrastructure Security Task Force (AMI-SEC), *AMI System Security Requirements V1.01*, 12/17/2008.
- 9 Department of Defense Instruction Number 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003.

Chapter 7

Industrial Automation and Control System Security Training

Chapter 6 presented the application of standards and guidelines to industrial automation and control system security and subsequently developed a foundation of security controls that are effective in reducing risk and protecting these systems. Chapter 7 reinforces these concepts by developing automation and control system security training concepts, training sources, and templates for designing and generating such programs.

Background

Training for industrial automation and control system security is addressed in many different formats, philosophies, levels, and degrees of formality. Some automation and control system security issues are covered peripherally in IT-based information system security courses; others are covered in depth in courses aimed at control system engineers and technicians; and still others are somewhere in between.

Until recently, there has been a dearth of high-quality courses focused primarily on industrial automation and control system security. Most courses offered by various bodies were heavily focused on information system security and paid little attention to real-time systems used to control the nation's manufacturing facilities, process plants, and critical infrastructure. Because of the threat of terrorism and increased concerns of natural disasters and the demands of a growing population, focus is shifting from purely information system security to the security of automation and control systems within governmental agencies, educational institutions, and private training organizations.

Training in the field of securing industrial automation and control systems is critical to supporting the goals of protecting the nation's manufacturing and process industry base and its critical infrastructure by building a cadre of trained personnel, maintaining technological leadership, developing advanced security-related hardware and software, and raising awareness of threats to national security.

With these goals in mind, key issues are who should be responsible for such training and for what level the training should be designed. In organizations, specific individuals should be assigned the responsibility of training employees involved with the security of automation and control systems as well as vendors and outside contractors. Some of the major sources and methods of training for automation and control systems security are presented in the following sections of this chapter.

Training Sources and Approaches

Some of the useful industrial automation and control system training programs and related initiatives that are available include the following:

- Idaho National Laboratory (<http://www.inl.gov/scada>)
- Sandia National Laboratories (http://energy.sandia.gov/?page_id=6912)
- ISA (www.isa.org/training)
- US-CERT (http://www.us-cert.gov/control_systems)
- SANS (<http://www.sans.org/security-resources/>)
- National Initiative for Cybersecurity Education (NICE) (<http://nist.gov/nice>)
- National Security Agency (NSA) and the Department of Homeland Security (DHS) National Centers of Academic Excellence

Idaho National Laboratory

The Idaho National Laboratory, along with the Sandia National Laboratories, is home to the National SCADA Test Bed (NSTB) Program. This program was established by the U.S. Department of Energy and is focused on ensuring the “secure, reliable and efficient distribution of power.”

As described on its Web site, the NSTB program is chartered to perform the following functions:

- Assess selected control systems and control system components to identify cyber vulnerabilities. Testing is planned and conducted in collaboration with the interested industry partner and may be performed in the laboratory (test bed) environment or at the partner’s site.
- Provide control system security training through workshops that describe common cyber vulnerabilities found in control

systems and effective methods for mitigation.

- Share with appropriate standards organizations information that can be used to support the development of improved industry standards applicable to control system security.
- Participate in conferences that include control system security topics to share information obtained through system assessments and analyses.

Relative to SCADA, the Idaho National Laboratory training is aimed at “IT/control system managers, IT/control system security personnel, network and control system support engineers, and control system designers and developers who are involved in or responsible for control system cybersecurity.” The course offerings are:

•**Introductory SCADA Security** (4 hours), comprising:

- SCADA Network Communications Overview
- Common Vulnerabilities of Control Systems
- Inadequate Policies and Procedures
- Poorly Designed Control System Networks
- Misconfigured or Unpatched Operating Systems and Embedded Devices
- Inappropriate Use of Wireless Communication
- Inadequate Authentication of Control System Communications
- Inadequate Identification and Control of Access to Control System
- Lack of Detection and Logging of Intrusion
- Dual Use of Control System Networks
- Lack of Security Checking of Control System Software/Applications
- Lack of Change Management/Change Control Procedures and Agreements
- Potential Mitigation Strategies based on multiple levels of implementation

•**Intermediate SCADA Security** (8 hours), covering the following material:

- General Security Observations and Pitfalls

- SCADA Network Communications Overview
- Potential SCADA Network Entry Points and Defenses
- SCADA Network Scanning and Vulnerability Identification (in a safe manner)
- Network Monitoring and Simple Intrusion Detection
- Dissecting SCADA Protocols
- Common Programming Pitfalls
- Modern Hardware and OS Mitigation Strategies
- Incident Response Essentials for the SCADA Community
- Advanced SCADA Security Red/Blue Team** (5 days), with the following topics similar to those covered in Intermediate SCADA Security, but with hands-on exercises using SCADA equipment:
 - General Security Observations and Pitfalls
 - Control System Network Communications Overview
 - Potential Control System Network Entry Points and Defenses
 - Control System Network Scanning and Vulnerability Identification
 - Network Monitoring and Simple Intrusion Detection
 - Dissecting Control System Protocols
 - Common Programming Pitfalls
 - Modern Hardware and OS Mitigation Strategies
 - Incident Response Essentials for the Control System Community

The Sandia National Laboratories

The Sandia National Laboratories offer a course on SCADA assessment titled “Methodologies for Assessing SCADA Systems and an Overview of Related Security and Vulnerability Concerns.” This course is offered “at Sandia’s discretion to individuals with need-to-know and by invitation.” The course is customizable and includes the following areas:

- SCADA and Other Digital Control System Uses in Infrastructures and Industry

- Vulnerabilities in SCADA Components and Systems
- Methodologies and Tools to Assess SCADA Systems in a Successful, Measurable, and Reproducible Manner

ISA

The International Society of Automation (ISA) offers a number of courses on securing industrial automation and control systems, including the following:

•Industrial Networking & Security, covering the following topics:

- TCP/IP Networking Over Ethernet, Over Serial Links (PPP) and Through Other Networks
- Making Networks Reliable: Redundancy/Name Services/Fault Tolerance/Spanning Tree
- Secure Architectures: Layering Based on Function, Firewall Placements, Use of DMZs, Patch/Virus Update Management
- Understanding Packets and Protocols: Understanding IP, TCP and UDP and Application Protocols
- Building a Plant Floor Web Server Using HTML, XML, Client/Server Side Scripting
- Network Security Issues: Risks and Vulnerabilities | Attack Methods and Technologies
- Applying: Virus Protection | Firewall Basics | Encryption Basics
- Advanced Security: VPN Technology and Application, VLAN Technology and Application, Static/Dynamic Routing
- Firewall Technology: Basic/Advanced, ACL Definitions, Stateful Inspection, HIDS/NIDS
- User Authentication: Strong Authentication, Password Strategies, Multifactor, Centralized Policy Management
- Practical Industrial Intranet Applications Using ISA-99 Recommendations and Standards

•Using ANSI/ISA-99 to Secure Your Control System, with the following topics:

- Understanding the Current Industrial Security Environment: What Is Electronic Security for Industrial Automation and Control Systems? | How

IT and the Plant Floor Are Different and How They Are the Same

- How Cyberattacks Happen: Understanding the Threat Sources | The Steps to Successful Cyberattacks
- Creating A Security Program: Critical Factors for Success | Understanding ISA-99 Part 2: Establishing an Industrial Automation & Control Systems Security Program
- Using ISA-99: Risk Analysis: Business Rationale | Risk Identification, Classification, and Assessment | The DNSAM Methodology
- Using ISA-99: Addressing Risk with Security Policy, Organization, and Awareness: CSMS Scope | Organizational Security | Staff Training and Security Awareness
- Using ISA-99: Addressing Risk with Selected Security Countermeasures: Personnel Security | Physical and Environmental Security | Network Segmentation | Access Control
- Using ISA-99: Addressing Risk with Implementation Measures: Risk Management and Implementation I System Development and Maintenance I Information and Document Management
- Using ISA-99: Monitoring and Improving the CSMS: Compliance and Review | Improve and Maintain the CSMS

•Advanced Industrial Cybersecurity, focusing on the following subjects:

- TCP/IPV6 Networking: Over Ethernet | Over Serial Links (PPTP) | Using other Industrial Protocols
- Converting from IPV4 to IPV6 without Causing Security Problems
- Making Networks Secure: Local, Global, and Organizational Policies
- COTS OS: Vulnerabilities and Hardening Techniques
- Security/Performance Problems Associated with Patch/Virus Update Management
- Secure Architectures: Layering Based on Function and on Firewall/VPN Placements

- Building a Secure Plant Floor Web Server: HTML | XML
| Methods to Enhance Security
- Network Security Issues: Risks and Vulnerabilities |
Attack Methods and Technologies
- Applying: IPS/Virus Protection/Access-ACLs |
Identification/Authentication/Nonrepudiation
- Network Security: VPN Technology and Application |
VLAN Technology and Application | Managed
Switch/Router Configuration
- Security Management: Access, Strong Authentication,
Password Strategies, Multifactor, Centralized Policy
Management
- Practical Cybersecurity Applications: ANSI/ISA-99 |
NIST | NCSDOCIPEP | DHS | DOE | CPNI

•**Cybersecurity for Automation, Control, and SCADA Systems,**
which includes the following subjects:

- Defining Industrial Cybersecurity
- Risk Assessment
- Threats and Vulnerabilities
- Security Policies, Programs, and Procedures
- Understanding TCP/IP, Hackers, and Malware
- Technical Countermeasures
- Architectural & Operational Strategies

•**Introduction to Industrial Automation Security and the ANSI/ISA-99 Standards,** covering the following areas:

- Understanding the Current Industrial Security
Environment: What Is Electronic Security for
Industrial Automation and Control Systems? |
Trends in Security Incidents
- How IT and the Plant Floor Are Different and How
They Are the Same
- Current Security Standards and Practices
- Creating a Security Program: Critical Factors for
Success | Understanding ISA-99 Part 2: Establishing
an Industrial Automation and Control Systems
Security Program
- Using ISA-99: Risk Analysis: Business Rationale | Risk

Identification, Classification, and Assessment

- Using ISA-99: Addressing Risk with Security Policy, Organization, and Awareness: CSMS Scope | Organizational Security | Staff Training and Security Awareness | Business Continuity Plan | Security Policies and Procedures
- Using ISA-99: Addressing Risk with Selected Security Countermeasures: Personnel Security | Physical and Environmental Security | Network Segmentation | Access Control: Account Administration, Authentication, and Authorization
- Using ISA-99: Addressing Risk with Implementation Measures: Risk Management and Implementation | System Development and Maintenance | Information and Document Management | Incident Planning and Response
- Using ISA-99: Monitoring and Improving the CSMS: Compliance and Review | Improve and Maintain the CSMS

US-CERT

The United States Computer Emergency Response Team (US-CERT) offers the following instructor-led courses:

- Introduction to Control Systems Cybersecurity** – Introduces participants to industrial control system fundamentals and comparisons of IT and control system architectures. The elements of the course are:
 - Cybersecurity Landscape: Understanding the Risks
 - Industrial Control Systems Applications
 - Current State of Cybersecurity in Industrial Control Systems
 - Practical Applications of Cybersecurity
- Industrial Control System Security (ICS) for Management** – Provides background and basic understanding of the current industrial control system cybersecurity landscape for managers. The course includes the following topics:
 - Overview of the Elements of the Risk Equation and How It Applies to Cybersecurity of an ICS
 - Threats to an ICS and Its Components

–Tools That Can Be Used to Help Mitigate the Cybersecurity Risk

•**Intermediate Cybersecurity for Industrial Control Systems**

Part 1 – Consists of technical instruction on the protection of industrial control systems using offensive and defensive methods. The material includes:

- Current Security in ICS
- Strategies Used Against ICS
- Defending the ICS
- Preparation and Further Reading for Part 2

•**Intermediate Cybersecurity for Industrial Control Systems**

Part 2 – Hands-on training with laboratory exercises to impart knowledge of how attacks against control systems are launched and succeed. The course topics include:

- Supervisory Control and Data Acquisition (SCADA) and Control System Overview
- Risk to Industrial Control Systems
- Exploit Demonstration
- Basic Control Security Considerations
- Network: Security, Identification, and Remediation
- Network: Defense, Detection, and Analysis

•**ICS Advanced Cybersecurity** – Includes hands-on training on protecting and securing industrial control systems from cyber attacks, including a Red Team/Blue Team exercise that will be conducted within an actual control systems environment. The course comprises the following subjects:

- Overview of the DHS Control Systems Security Program
- Review of Cybersecurity for Industrial Control Systems
- Demonstration Showing How a Control System Can Be Attacked from the Internet
- Hands-on Classroom Training on Network Discovery Techniques and Practices
- Hands-on Classroom Training on Network Exploitation, Network Defense Techniques and Practices
- A 12-Hour Exercise where Participants are Either Attacking (Red Team) or Defending (Blue Team)

–Red Team/Blue Team Exercise Lessons Learned and Round-Table Discussion

SANS

The SANS organization offers an advanced SCADA security hands-on training course aimed at administrators and automation system personnel. The material addresses vulnerabilities and risks to SCADA systems, effects on enterprise security, the use of open source security tools, and testing methods. The course subject areas include the following:

- Review of Industrial Control Systems (ICS), Operating System Kernels, and Network Security SCADA Penetration Testing
- SCADA Vulnerability Assessment methodology
- SCADA Vulnerability Analysis
- Embedded Device Fuzzing (an attack using random, malformed, or bad data)
- Protocol Analysis
- Methods for Compromising and Dissecting Common Security Controls Found in ICS Environments

The National Initiative for Cybersecurity Education

The National Initiative for Cybersecurity Education (NICE) is a partnership of government, industrial, educational, and professional organizations with the mission “to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population.” The specific goals of NICE are to:

- 1.Raise awareness among the American public about the risks of online activities
- 2.Broaden the pool of skilled workers capable of supporting a cyber-secure nation
- 3.Develop and maintain an unrivaled, globally competitive cybersecurity workforce

The National Institute of Standards and Technology (NIST) has been assigned the lead in the NICE initiative and will coordinate the government activities involving the Department of Homeland Security (DHS), the Department of Defense (DoD), the Department of Education (ED), NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the Office of Personnel Management (OPM).

The objectives¹ defined by NICE to achieve the desired strategic goals include the following:

- 1.Improve citizens' knowledge to allow them to make smart choices as they manage online risk
- 2.Improve knowledge of cybersecurity within organizations so that resources are well applied to meet the most obvious and serious threats
- 3.Enable access to cybersecurity resources
- 4.Improve K-12 science, technology, engineering, and mathematics (STEM) education, emphasizing the important role of mathematics and computational thinking
- 5.Increase the quantity and quality of academic computer science courses in high schools
- 6.Increase the quantity and quality of undergraduate and graduate cybersecurity curricula for students in computer science and, more broadly, IT and security-related degree programs
- 7.Incentivize, support, and recognize excellence in graduate-level cybersecurity research and development
- 8.Develop a usable cybersecurity competency framework (human resources and curriculum focus)
- 9.Provide a framework for focusing on cybersecurity training to meet evolving needs
- 10.Study the application of professionalization, certification, and licensing standards on cybersecurity career fields

In order to advance its objectives, NICE has published a draft document, the *NICE Cybersecurity Workforce Framework*, which classifies the typical duties and skill requirements of cybersecurity workers. This framework was developed because cybersecurity professionals often do not fit into standard job descriptions and titles. (<http://csrc.nist.gov/nice/framework/>)

The NICE Cybersecurity Workforce Framework develops a vocabulary that can be used by any type of organization. It organizes cybersecurity work into the following categories:

- Design
- Operation
- Maintenance

- Incident response
- Information gathering
- Analysis

In another initiative, NIST, the U.S. Department of Education, NICE, and the National Cybersecurity Education Council (NCEC) are developing a strategic public-private partnership to promote formal cybersecurity education. The effort is designed to support the NICE goal of broadening the pool of skilled workers capable of supporting a cyber-secure nation. In order to accomplish this goal, the partnership is collaborating with state and local governments to establish and support formal cybersecurity education programs for kindergarten through 12th grade and for higher education and vocational programs.

National Security Agency (NSA) and the Department of Homeland Security (DHS) National Centers of Academic Excellence

NSA and the Department of Homeland Security (DHS) are sponsors of the National Centers of Academic Excellence initiative. This program has the goal of reducing vulnerabilities in the national information infrastructure. In order to accomplish this goal, National Centers of Academic Excellence are established in educational institutions to promote research and education in information assurance (IA). The students graduating from these institutions with training and research experience in information assurance will be able to apply their skills to securing the nation's infrastructure and information systems.

Institutions can be designed as National Centers of Academic Excellence (CAE) in IA Education (CAE/IAE) and Research (CAE-R) programs. The designations have terms of five years, after which the institution must successfully reapply in order to retain its CAE designation.

Applicants for a National Center of Academic Excellence in IA Education designation are four-year colleges and graduate-level universities and must pass a stringent evaluation and review. To apply for designation of a National Center of Academic Excellence in research, the college or university must meet the Carnegie Foundation's classifications of Research University/Very High (RU/VH), Research University/High (RU/H) and Doctoral Research University (DRU) or the equivalent.

Training Support Guidelines

There are a number of documents that can provide guidance in setting up and

conducting training applicable to industrial automation and control systems. Two of the important ones are reviewed here to provide a general understanding of their content and capabilities. These publications are:

- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (<http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>)
- NIST SP 800-16 Revision 1, *Information Security Training Requirements: A Role- and Performance-Based Model* (Draft) (<http://csrc.nist.gov/publications/drafts/800-16-rev1/Draft-SP800-16-Rev1.pdf>)

NIST Special Publication 800-50

NIST Special Publication 800-50², *Building an Information Technology Security Awareness and Training Program*, provides guidance in developing and conducting information system security training. The document is aimed at IT security, but it is useful in supporting automation and control system security awareness and training in that it provides useful principles that can be used in setting up such programs.

The publication describes the following four critical steps in the life cycle of a security awareness and training program:

- 1.Awareness and Training Program Design** – Needs assessment is conducted and a training strategy is developed and approved. This strategic planning document identifies implementation tasks to be performed in support of established security training goals.
- 2.Awareness and Training Material Development** – Available training sources, scope, content, and development of training material, including solicitation of contractor assistance if needed, are addressed.
- 3.Program Implementation** – Effective communication and rollout of the awareness and training program are conducted. It also addresses options for delivery of awareness and training material (Web-based, distance learning, video, on-site, etc.).
- 4.Post-Implementation** – Guidance on keeping the program current and monitoring its effectiveness is provided. Effective feedback methods are described (surveys, focus groups, benchmarking, etc.).

The document also defines the following three common models used in managing a security training function:

- Centralized** – All responsibility resides with a central authority.
- Partially Decentralized** – Policy and strategy lie with a central authority, but implementation responsibilities are distributed.
- Fully Decentralized** – Only policy development resides with a central authority, and all other responsibilities are delegated to individual organizational components.

NIST SP 800-50 also provides a useful perspective of learning as a continuum, going from awareness, to training, to education, as shown in [Figure 7-1](#).

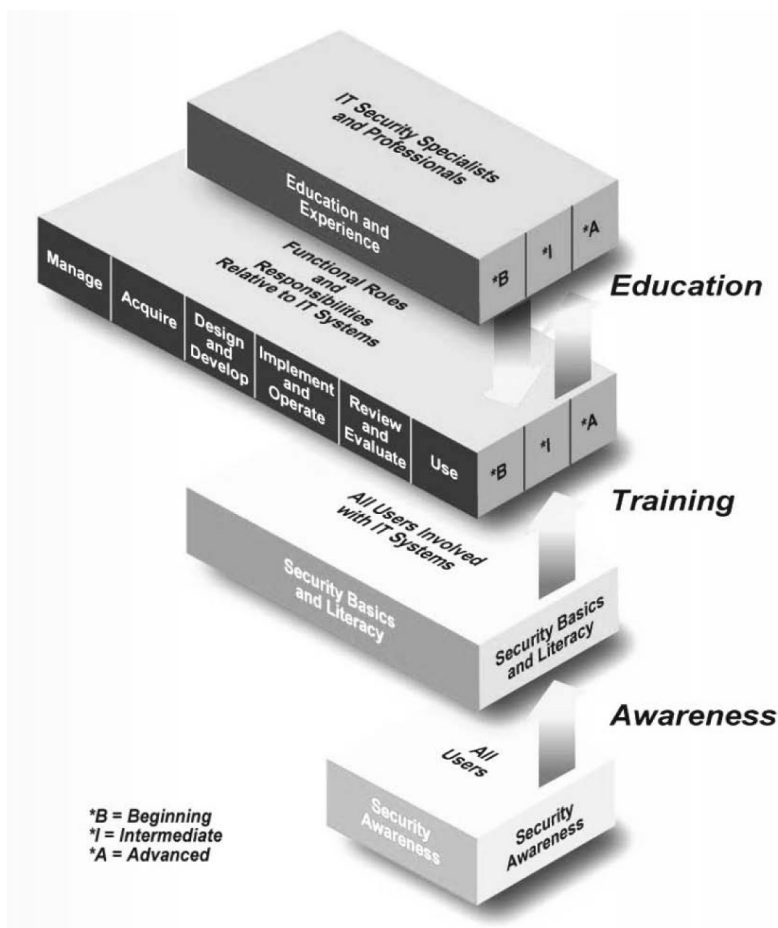


Figure 7-1. Security Learning Continuum

[Source: NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October, 2003.]

NIST SP 800-50 discusses the differences among awareness, training, and education as:

- Awareness** – Focuses attention on security
- Training** – Strives to produce relevant and needed security skills and competencies
- Education** – Integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and strives to produce IT security specialists

This publication provides additional details on implementing awareness and training that can be applied to industrial automation and control systems.

NIST Special Publication 800-16

NIST SP 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model (Draft)*,³ complements NIST SP 800-50. As shown in [Figure 7-1](#), it defines learning as a continuum, beginning with awareness, transitioning to training, and then moving into education. The model is role-based in that it “defines the information security learning needed as a person assumes different roles within an organization and different responsibilities in relation to information systems.” NIST SP 800-16 expands on the continuum as follows:

- 1.**Basic Security Awareness** – Required for employees, including contractor employees who are involved in any way with information systems.
- 2.**Awareness Training (Basics and Literacy)** – A transitional stage between basic awareness and role-based training. It provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.
- 3.**Role-Based Training** – Focuses on providing the knowledge, skills, and abilities specific to an individual’s roles and responsibilities relative to information systems. At this level, training recognizes the differences between beginning, intermediate, and advanced skill requirements.
- 4.**The Education Level** – Focuses on developing the ability and vision to perform complex multidisciplinary activities and the skills needed to further the information security profession and to keep pace with threats and technology changes.
- 5.**Professional Development** – Intended to ensure that users, from beginner to the career security professional, possess a

required level of knowledge and competence necessary for their roles. Professional development validates skills through certification and advanced education.

To implement instructional design, NIST SP 800-16 presents the five-phase ADDIE Instructional Design Model, which comprises the phases of analysis, design, development, and implementation and evaluation. The model is illustrated in [Figure 7-2](#).

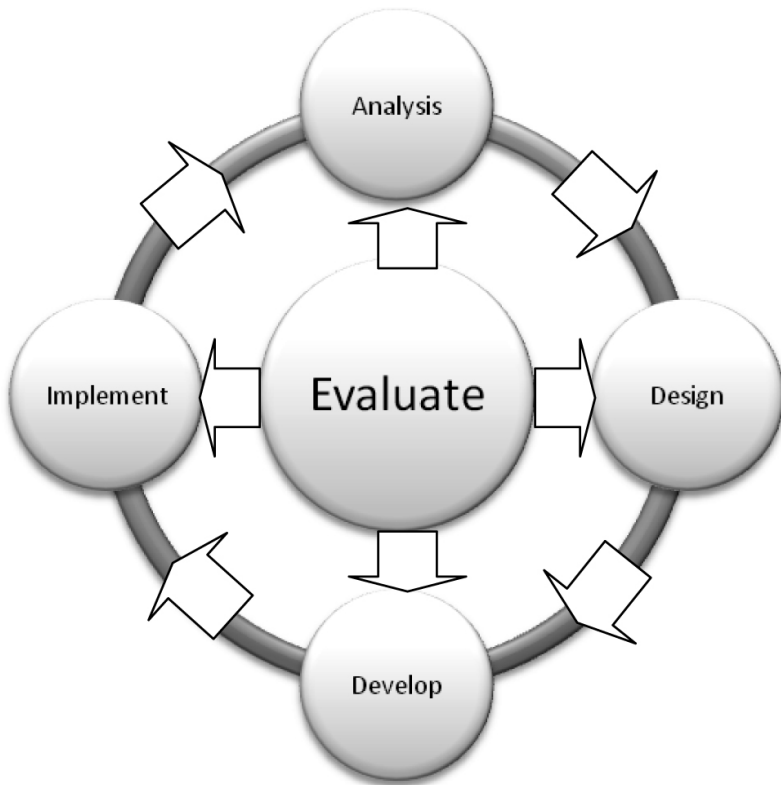


Figure 7-2. DDIE Instructional Design Model

[Source: NIST Special Publication 800-16 Revision 1, *Information Security Training Requirements: A Role- and Performance-Based Model* (Draft), March 2009.]

The five phases of the instructional design model consist of the following activities:

- 1.The Analysis Phase** – Compiles an inventory of all tasks associated with each role and conducts a needs assessment

to select those tasks for which training needs to be developed. Task descriptions can usually be found in position descriptions, performance plans, assignment letters, system security plans, and directives, or can be determined through interviews with current practitioners. These tasks should yield:

- The knowledge level required
- The desired behavioral outcomes
- Performance measures for each task

In addition, prerequisite knowledge should be determined.

2.The Design Phase – Develops the learning objectives for each of the tasks defined during the analysis phase. Then, the steps required to accomplish each objective have to be identified. The design phase consists of the following steps:

- Develop learning objectives (enabling and terminal)
- Identify and list steps required
- Develop performance/knowledge tests
- Develop required entry behaviors (optional)
- Sequence learning objectives

3.The Development Phase – Identifies and lists the activities that will help the training recipients achieve each objective (e.g., lecture, simulation, role-play, demonstration, lab exercise, table-top exercise). These activities are then used to select the appropriate delivery method(s). The steps of the development phase are summarized as follows:

- List activities required for each objective
- Select appropriate delivery method(s)
- Gather reference material
- Review existing course material
- Develop course material
- Develop lesson plans and instructor guide
- Conduct expert review of course materials

4.The Implementation Phase – Tests a draft version of the course or module to a selected audience for feedback. Adjustments

are then made as required. The steps in this phase are:

- Pilot course to hand-picked audience
- Make course adjustments
- Train the trainer (if required)
- Full-scale delivery

5.The Evaluation Phase – Conducts formative and summative evaluations, described as follows:

- Formative – During all phases, analysis, design, development, and implementation, a formative analysis evaluates if what is being taught is what was intended to be taught.
- Summative – Evaluates if the student was satisfied with the course and instructor, if the student achieved his or her objectives, if supervisors of the students felt the student was a more effective employee as a result of the course, and if the training program is providing the types of courses that are most needed.

NIST SP 800-16 also provides templates for training modules that provide a roadmap for teaching the module. [Figure 7-3](#) illustrates a typical module.

Common Training Subjects

In reviewing the courses and training programs discussed in this chapter, a common set of topics can be extracted to use as a basis for training in the security of industrial automation and control systems. These proposed core topics are summarized in [Table 7-1](#).

INFORMATION SECURITY TRAINING
Curriculum Module
Security Program (2.2D)

Training Area: **Management**
Responsibility: **Implement & Operate**

Definition — The implementation and use of organizational structures and processes for information security program goal-setting, prioritizing, and related decision-making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.

Behavioral Outcome — Individuals who are responsible for the implementation and daily operations of an information security program have a sufficient understanding of the appropriate program elements and requirements to be able to apply them in a manner which provides adequate and appropriate levels of protection for the organization's IT resources.

Knowledge Levels —

1. Beginning — Identify, Understand, Apply
2. Intermediate — Interpret, Analyze, Decide
3. Advanced — Investigate, Approve, Direct

Terminal Learning Objectives —

At the conclusion of this module, individuals will be able to:

1. Beginning — Apply organization-specific information security program elements to the implementation of the program and identify areas of weakness.
2. Intermediate — Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risks.
3. Advanced — Direct the implementation of appropriate operational structures and processes to ensure an effective information security program.

Applicable Roles (minimum) —

Senior Information Resources Management Official		
Chief Information Officer		Program and Functional Managers
System Administrator	Internal Auditor	System Owner
Information Resources Manager		Information System Security Officer
Network Administrator		Security Administrator
Senior Agency Information Security Officer/Manager and Staff		
Assessor		Incident Response Coordinator

INFORMATION SECURITY TRAINING TOPICS

1. Laws and Regulations
2. Information Security Program
3. System Environment
4. System Interconnection
5. Information Sharing
6. Security Objectives
7. Risk Management
8. Management Controls
9. Acquisition/Development/Installation/Implementation Controls
10. Operational Controls
11. Awareness, Training, and Education Controls
12. Technical Controls

RESOURCE DOCUMENTS

NIST SP 800-12
NIST SP 800-100

Figure 7-3. Example instructional module

[Source: NIST Special Publication 800-16 Revision 1, *Information Security Training Requirements: A Role- and Performance-Based Model* (Draft), March 2009.]

Table 7-1. Industrial Automation and Control System Core Topics

Topic	Description
Security Policies and Procedures	
NIST SP 800-19, Applicable Standards and Guidelines	
Risk Analysis and Mitigation	
SCADA/PLC/Network C, Windows, etc.	
Vulnerability Control Systems, Intrusion Detection, and Threat Sources	
Modbus, Control, and Authentication for Control Systems	
Logging of system and security events, intrusions, and abnormal activity	
Change Management Procedures	
Typical SCADA/PLC/Network C	
Application of Control Systems, Windows, COTS OS	
Security Awareness Training	Security awareness training conducted in accordance with security policy
Incident Response	Respond to incidents in an automation environment
Encryption Methods	Encryption methods in an automation/control environment

Summary

Training in the area of industrial automation and control system security is now offered by a variety of sources and types of institutions, including secondary schools, universities, industry, technical societies, community colleges, governmental bodies, and technical schools. This type of training was not always as available as it is now, which is the result of increased awareness of threats against automation and control systems that are critical to the nation.

This chapter reviewed some of the more prominent training programs and their content. In addition, governmental and NIST recommendations and guidelines applicable to conducting automation and control system-related training were presented to provide a basis for developing effective programs in this area. The chapter concluded with a proposed listing of fundamental cybersecurity topics for automation and control system security that can be used as a foundation for automation system-based training. [Chapter 8](#) will explore what the future holds for security in the realm of industrial automation and control systems.

Review Questions for Chapter 7

1. What organizations host the National SCADA Test Bed (NSTB) program?
 - a. NIST and the NSA
 - b. The Idaho National Laboratory and the Sandia National Laboratories
 - c. ISA and SANS
 - d. US-CERT and NIST

2. Which of the following is NOT a function of the National SCADA Test Bed (NSTB)?
 - a. Assess selected control systems and control system components to identify cyber vulnerabilities
 - b. Develop new standards and guidelines for governmental agencies
 - c. Provide control system security training through workshops that describe common cyber

vulnerabilities found in control systems

- d.Share with appropriate standard's organizations information that can be used to support the development of improved industry standards applicable to control system security

3.What organization developed and teaches the application of 99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*?

- a.SANS
- b.NIST
- c.ISA
- d.NSA

4.In a training program hands-on exercise, what is the function of the Red Team?

- a.Mitigating
- b.Scanning
- c.Defending
- d.Attacking

5.In a training program hands-on exercise, what is the function of the Blue Team?

- a.Defending
- b.Attacking
- c.Scanning
- d.Mitigating

6.What is fuzzing?

- a.Modifying memory locations
- b.An attack using random or malformed bad data
- c.Scanning to determine vulnerabilities
- d.Responding to an attack by counterattacking

7.The National Initiative for Cybersecurity Education (NICE) is a partnership

of government, industrial, educational, and professional organizations. Which of the following is NOT one of the goals of NICE?

- a.Raise awareness among the American public about the risks of online activities
- b.Broaden the pool of skilled workers capable of supporting a cyber-secure nation
- c.Develop and maintain an unrivaled, globally competitive cybersecurity workforce
- d.Develop secure digital control systems

8.Which of the following organizations is NOT a participant in the NICE initiative?

- a.NIST
- b.NASA
- c.Department of Homeland Security (DHS)
- d.NSA

9.The NICE Cybersecurity Workforce Framework develops a vocabulary that can be used by any type of organization in categorizing cybersecurity work. Which of the following is NOT a category in this framework?

- a.Penetration testing
- b.Design
- c.Operation
- d.Maintenance

10.The U.S. National Centers of Academic Excellence initiative is sponsored by which of the following organizations?

- a.NIST and the Department of Energy
- b.SANS and the Department of Education
- c.NSA and the Department of Homeland Security
- d.The Department of Defense and the US-CERT

11.The designation of an institution as a National Center of Academic Excellence has a duration of how many years before the institution has to reapply?

- a. Two years
- b. Ten years
- c. Five years
- d. Seven years

12. Which of the following is NOT one of the critical steps in the life cycle of a security awareness and training program as described in NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*?

- a. Awareness and training program design
- b. Program implementation
- c. Post-implementation
- d. Pre-implementation needs review

13. Which of the following is NOT one of the three common models used in managing a security training function as described in NIST Special Publication 800-50?

- a. Centralized
- b. Partially Decentralized
- c. Partitioned
- d. Fully Decentralized

14. According to NIST SP 800-50, learning is a continuum comprising which of the following elements?

- a. Awareness, skill, knowledge
- b. Awareness, training, education
- c. Training, education, skill
- d. Education, awareness, skill

15. NIST SP 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model (Draft)*, defines the following as what type of training?

“Focuses on providing the knowledge, skills, and abilities specific to an individual’s roles and responsibilities relative to information systems. At this level, training recognizes the differences between beginning,

intermediate, and advanced skill requirements.”

- a.Role-based training
- b.Task-oriented training
- c.Responsibility training
- d.Knowledge and skills training

16.Which one of the following is NOT one of the five phases of the industrial design model described in NIST SP 800-16?

- a.Analysis
- b.Training
- c.Design
- d.Evaluation

17.What are the two types of evaluations in the evaluation phase of the industrial design model described in NIST SP 800-16?

- a.Formative and summative
- b.Formative and intuitive
- c.Summative and descriptive
- d.Descriptive and formative

References

- ¹ *National Initiative for Cybersecurity Education Strategic Plan* (Draft), “Building a Digital Nation,” August 11, 2011.
- ² NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.
- ³ NIST Special Publication 800-16 Revision 1, *Information Security Training Requirements: A Role- and Performance-Based Model* (Draft), March 2009.

Chapter 8

Future Industrial Automation and Control System Approaches and Issues

Chapter 7 emphasized the importance of training to the cybersecurity of industrial automation and control systems. It pointed out sources of that training, identified government and industrial initiatives in promoting security awareness and training, and reviewed effective methodologies for implementing a cybersecurity training program applicable to industrial automation and control systems. *Chapter 8* looks into future trends and methodologies that will affect automation and control systems and provides guidelines for taking advantage of these developments.

Automation and Control System Trends

Because industrial automation and control systems are complex, their future characteristics will be affected by advances in a number of domains. These domains include hardware, software, virtualization, storage, mobile devices, cloud computing, communications, HMI, networking, encryption, security, artificial intelligence, standards, and robotics. Advances in these technologies will influence capabilities, performance, reliability, trustworthiness, cost, maintenance, training, and rates of adoption. In addition, increased and more stringent regulatory requirements will require increasing effort and result in higher costs to meet compliance, traceability, environmental, and legal obligations.

Software, hardware, and the control systems that use them will be more adaptable, more secure, more efficient, and self-healing as improvements in these areas are made. Some of the important elements that will characterize future software, hardware, and control systems are summarized in [Figures 8-1, 8-2, and 8-3](#), respectively.



Figure 8-1. Future software characteristics

It is interesting to note that there are some common threads implicit and explicit among these three areas. These commonalities include the following characteristics:

- Adaptive and self-organizing
- Self-diagnosis

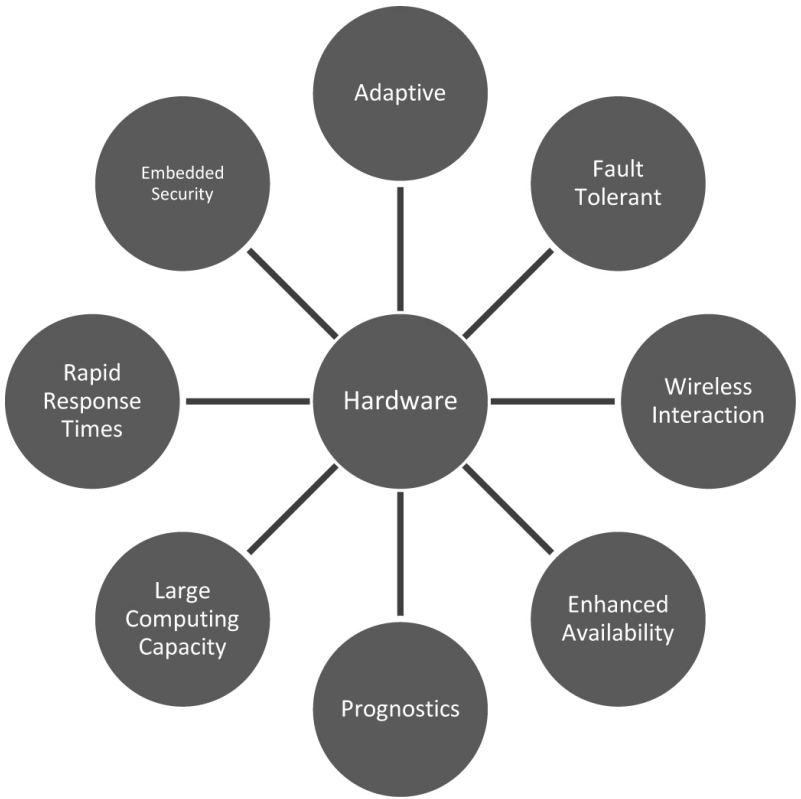


Figure 8-2. Future hardware characteristics



Figure 8-3. Future control system characteristics

- Fail soft
- Resilience
- Prognostics
- Enhanced availability
- Intrinsic security
- Availability of and adherence to standards
- Wide use of wireless technology
- Incorporation of Web-based and mobile devices
- Use of self-powered nanotechnology sensors and devices
- Higher-speed processing
- Agent-based (A software agent is a computer program that

performs tasks for a user using assumptions based on past behavior or defined preferences.)

- Reconfigurable

In the hardware realm, advances in chip technology will yield higher performance multi-core computing engines using less power than conventional single core designs. Processor workloads can be assigned to those cores with the highest power efficiency and those that are best able to complete the required processing. In addition, cores not needed can be powered down or run at diminished capacity to save energy. In order to take advantage of high performance, multi-core designs, software must be developed to support efficient partitioning of tasks among the cores and not waste the available capabilities of such systems. These capabilities will result in automation systems with faster response times, lower costs, increased computational power, and support for semi-autonomous operation.

The continuous improvement in tablet computers and intuitive HMIs (human-machine interfaces) will provide remote platforms from which to monitor and control processes as well as to conduct maintenance functions. Many of these functions will be performed wirelessly. Correspondingly, wireless security will have to keep pace to reduce or eliminate exposure to threats against mobile devices.

Another technology that will become increasingly important in industrial automation and control systems is virtualization. Virtualization is based on the concept of a virtual machine (VM) running on a physical computing platform under the control of a virtual machine monitor (VMM), known as a hypervisor. Virtualization reduces the effort required to maintain hardware and software systems by eliminating the binding of software to specific hardware platforms through the logical partitioning of physical computing resources into multiple execution environments, including servers, applications, and operating systems. Thus, applications can be centrally managed, and cybersecurity mechanisms can be distributed among virtualization servers, using virtual instances. The control and automation software applications and operating system no longer have to be individually installed and maintained on every client. A typical virtual server can support a variety of client instances on a single hardware platform through protocols, such as the remote desktop protocol (RDP). Additional advantages of virtualization are summarized as follows:

- Alarm management capabilities can be easily implemented to identify critical system situations or system errors.
- Clients can be deleted or added rapidly without affecting plant operation.
- Existing systems can be ported to different hardware platforms

with a minimum of effort.

- Software updates can be applied during system operation.

For cloud computing, virtualization provides a level of freedom of choice for the customer and efficiencies and cost savings for cloud providers. The migration to virtualized clouds will, in many instances, be initially through hybrid clouds while customers test and evaluate the cloud paradigm in the context of their own business requirements. As users become accustomed to employing cloud computing, they will embrace the ability to have large numbers of servers available on demand and, conversely, rapidly reducing the number of servers they are using when they are not required. Virtualization, if applied properly, can also result in minimal ramp-up times, reduction of time to develop and market applications, and rapid acquisition or reduction of resources, as requirements vary. Cloud computing was covered in detail in [Chapter 4](#).

Regarding virtualization security, conventional attacks such as denial of service can be used against VMs while other attacks exploit specific VM vulnerabilities. Because multiple VMs share the same physical hardware, a vulnerability in one VM can be exploited to attack other VMs or the host systems. Some of the vulnerabilities of the virtual environment include the following:

- Keystroke logging** – Logging of keystrokes and screen updates allows information to be passed across virtual terminals in the VM and written to host files, thus permitting the monitoring of encrypted terminal connections inside the VM
- One VM accessing another VM** – Monitoring of one VM by another VM using hacker techniques through a virtual hub or switch
- Shared clipboard technology** – Allows data to be transferred between VMs and the host, providing a means of moving data between malicious programs in VMs of different security realms
- Host VM monitoring** – Monitoring of network packets coming from or going to a VM by the host enables the host to affect the VM by the following actions and, if the host is compromised, in a negative way:
 - Adjusting the number of CPUs, amount of memory, amount and number of virtual disks, and number of virtual network interfaces available to a VM
 - Monitoring and configuring resources available to the VMs, including CPU, memory, disk, and network usage of VMs

- Monitoring the applications running inside the VM
- Starting, stopping, pausing, and restarting VMs
- Viewing, copying, and modifying data stored on the VM's virtual disks

Penetration Testing of Industrial Automation and Control Systems

With more assessment tools and methods for evaluating computer systems and networks being available in general, there will be increased pressure to apply these approaches to industrial automation and control systems in the future. One particularly effective vulnerability assessment method that is widely used and specified in many evaluation paradigms is penetration testing. However, penetration testing of industrial automation and control systems, if not properly conducted, can cause damage to these systems and disrupt operations. The commonly used penetration testing tools create additional traffic on automation and control systems and, if applied to such systems that have limited memory and processing capability, can severely impact their safety and performance. However, if done properly, penetration testing can provide valuable insight into the security posture of industrial automation and control systems.

Some useful guidelines for conducting penetration testing on automation and control systems are:

- Document and understand the automation/control system configuration to identify areas of high risk
- Identify all routes of access to the automation/control system from outside elements, including the corporate network
- Where possible, conduct testing on independent test systems in a controlled laboratory setting
- In laboratory test systems, ensure that intrusion detecting systems and firewall configurations are duplicates of those in the production system
- Evaluate testing procedures and approaches in a laboratory test setting before applying them to online production systems
- Understand the proper operation of the automation/control system to be tested in order to more effectively identify the results of attack scenarios
- Conduct testing on redundant automation/control system components
- Use passive data collection techniques when possible

- Be cognizant of risks when conducting testing on active, operational systems, and have recovery procedures in place in the event of a system failure caused by the testing
- Conduct penetration testing from computers external to the network to simulate an attacker's approach

A penetration test is usually conducted with no prior knowledge of the automation/control system, that is, with a “black box” approach. Penetration testing begins with a reconnaissance phase comprising the following steps:

- Footprinting – Gathering information about the target automation/control network in order to develop a mapping of the network and associated systems
- Scanning – Conducting a scan of the network to discover applications and open ports, services running on ports, and information about the operating system
- Enumerating – Using the results of the scanning phase to develop a complete map of the network, discover vulnerable resources, and identify valid user accounts

Following reconnaissance, the network can be assessed for vulnerabilities by acquiring access to the automation/control system. If an attack was launched on the system, the acquiring access phase is where the actual attack is implemented. In this phase, an attacker could access the operating system and network, obtain higher-level system privileges, launch buffer overflow and denial of service attacks, and insert viruses and Trojan horses.

Some of the common assessment tools used in penetration testing include Nmap, Metasploit, Nessus, STAT Scanner, Wireshark, Ettercap, and software debuggers.

Formal Methods Used to Quantify and Standardize Important Concepts and Applications

In many fields, as advances occur, formal methods evolve to quantify and standardize important concepts and applications. Three such methods that can be applied to industrial automation and control systems are information security continuous monitoring (ISCM), the Smart Grid maturity model (SGMM), and the automation maturity model (AMM).

ISCM Strategy

NIST SP 800-137¹, *Information Security Continuous Monitoring (ISCM) for*

Federal Information Systems and Organizations, defines the process for developing an ISCM strategy and implementing an ISCM program. ISCM is defined as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.”

ISCM comprises the following steps:

1. **Define** an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
2. **Establish** an ISCM program, determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
3. **Implement** an ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.
4. **Analyze** the data collected and report findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.
5. **Respond** to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
6. **Review and Update** the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization’s information infrastructure, and increase organizational resilience.

The ISCM process is depicted in [Figure 8-4](#).

In the ISCM process, the status of automation security in a facility can be determined by establishing appropriate metrics. The metrics are defined through the following activities:

- Maintaining an understanding of threats and threat activities
- Assessing all security controls
- Collecting, correlating, and analyzing security-related information

- Providing actionable communication of security status across all tiers of the organization
- Active management of risk by organizational officials

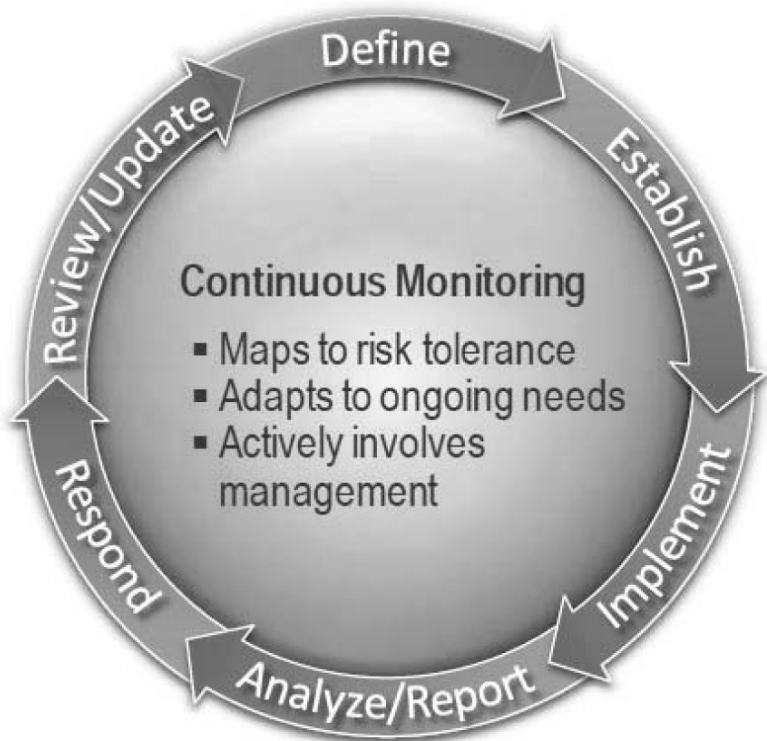


Figure 8-4. The ISCM Process

[Source: NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September, 2011.]

NIST SP 800-137 defines the process for managing information security and information system-related risk as the risk management framework (RMF). The RMF integrates information system security and risk management activities as illustrated in [Figure 8-5](#). It applies equally well to both automation and control systems and information systems.

The frequency of monitoring security controls for effectiveness and relevance is a function of the following criteria as presented in NIST 800-137:

- **Security control volatility** – Security control volatility is a

measure of how frequently a control is likely to change over time subsequent to its implementation. Volatile security controls are assessed more frequently, whether the objective is establishing security control effectiveness or supporting calculation of a metric.

- System categorizations/impact levels** – In general, security controls implemented on systems that are categorized as high-impact are monitored more frequently than controls implemented on moderate-impact systems, which are in turn monitored more frequently than controls implemented on low-impact systems.
- Security controls or specific assessment objects providing critical functions** – Security controls or assessment objects that provide critical security functions (e.g., log management servers, firewalls) are candidates for more frequent monitoring.
- Security controls with identified weaknesses** – Existing risks documented in security assessment reports are considered for more frequent monitoring to ensure that risks stay within tolerance.
- Organizational risk tolerance** – Organizations with a low tolerance for risk (e.g., organizations that process, store, or transmit large amounts of proprietary and/or personally identifiable information [PII], organizations with numerous high-impact systems, organizations facing specific persistent threats) monitor more frequently than organizations with a higher tolerance for risk.
- Threat information** – Organizations consider current credible threat information, including known exploits and attack patterns when establishing monitoring frequencies. For instance, if a specific attack is developed that exploits a vulnerability of an implemented technology, temporary or permanent increases to the monitoring frequencies for related controls or metrics may help provide protection from the threat.
- Vulnerability information** – Organizations consider current vulnerability information with respect to technology products when establishing monitoring frequencies. For instance, if a specific product manufacturer provides software patches monthly, an organization might consider conducting vulnerability scans on that product at least that often.
- Risk assessment results** – Results from organizational and/or system-specific assessments of risk (either formal or informal) are examined and taken into consideration when establishing monitoring frequencies. For instance, if a system-specific risk

assessment identifies potential threats and vulnerabilities related to nonlocal maintenance (NIST SP 800-53, MA-4), the organization considers more frequent monitoring of the records kept on nonlocal maintenance and diagnostic activities.

- Reporting requirements** - Reporting requirements do not drive the ISCM strategy but may play a role in the frequency of monitoring.

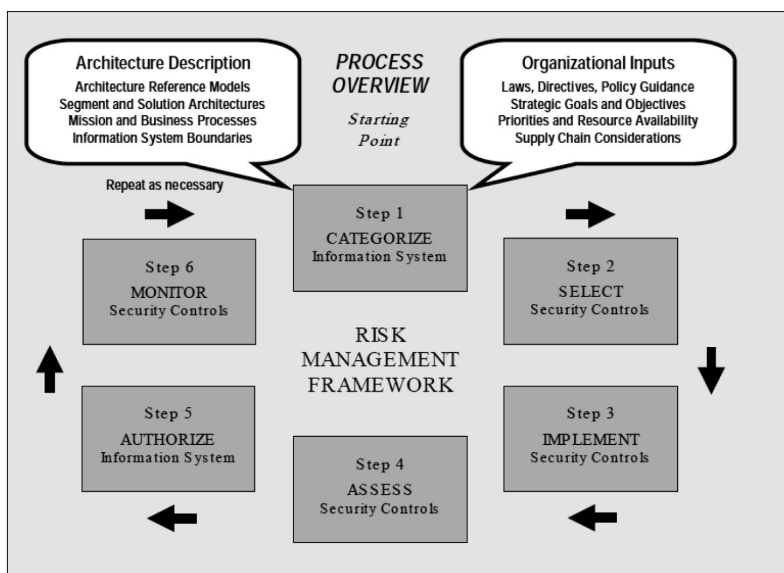


Figure 8-5. The Risk Management Framework

[Source: NIST SP 8GG-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September, 2G11.]

The ISCM process **Respond** step conducts a response to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection. In accordance with NIST SP 800-137, the **Respond** activity mitigation recommendations are developed using the *security automation domain* concepts presented in Appendix D of NIST SP 800-137. Note that the usage of the term “security automation domain” in the ISCM process is not the same as “automation and control system security” as conventionally used. Appendix D defines a security automation domain as “an information security area that includes a grouping of tools, technologies, and data. Data within the domains is captured, correlated, analyzed, and reported to present the security status of the organization that is represented by the domains monitored.” The 11 security automation domains that support continuous monitoring and that are used to

categorize the remediation recommendations are illustrated in [Figure 8-6](#).



Figure 8-6. The Security Automation Domains

[Source: NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September, 2011.]

Appendix D recommends sets of NIST SP 800-53 security controls that are applicable to the security automation domains. These controls are given in [Table 8-1](#).

Table 8-1. NIST SP 800-53 Security Controls Applicable to Security Automation Domains

Security Automation Domain
Software Assurance: SA-11, Developer Security Testing; and SI-11, Error Handling.
Vulnerability Management: CA-2, Patch Management; CA-7, Continuous Monitoring; CM-3, Configuration Change Control; IR-4, Incident Handling; IR-5, Incident Monitoring; MA-2, Controlled Maintenance; RA-5, Vulnerability Scanning; SA-11, Developer Security Testing; and SI-11, Error Handling.

Asset Management and Incident Management: Audit Records; AU-4, Audit Storage Capacity; AU-5, Response to Audit Processing Failures; AU-6, Audit Review, Analysis, and Reporting; AU-7, Audit Reduction and Report Generation; AU-8, Time Stamps; AU-12, Audit Generation; CA-2, Security Assessments; CA-7, Continuous Monitoring; IR-5, Incident Monitoring; RA-3, Risk Assessment; and SI-4, Information system Monitoring.

Malware Security Assessments: CA-7, Continuous Monitoring; IR-5, Incident Monitoring; RA-3, Risk Assessment; SA-12, Supply Chain Protection; SA-13, Trustworthiness; SI-3, Malicious Code Protection; SI-4, Information System Monitoring; SI-7, Software and Information Integrity; and SI-8, Spam Protection.

Asset Management: Monitoring; CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-4, Security Impact Analysis; CM-8, Information System Component Inventory; and SA-10, Developer Configuration Management.

Access Control Management: AC-3, Access Enforcement; AC-5, Separation of Duties; AC-7, Unsuccessful Login Attempts; AC-9, Previous Logon (Access) Notification; AC-10, Concurrent Session Control; AC-11, Session Lock; AC-19, Access Control for Mobile Devices; AC-20, Use of External Information Systems; AC-22, Publicly Accessible Content; CA-2, Security Assessments; CA-7, Continuous Monitoring; CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-5, Access Restrictions for Change; CM-6, Configuration Settings; CM-7, Least Functionality; IA-2, Identification and Authentication (Organizational Users); IA-3, Device Identification and Authentication; IA-4, Identifier Management; IA-5, Authenticator Management; IA-8, Identification and Authentication (Non-Organizational Users); IR-5, Incident Monitoring; MA-5, Maintenance Personnel; PE-3, Physical Access Control; RA-3, Risk Assessment; SA-7, User Installed Software; SA-10, Developer Configuration Management; and SI-2, Flaw Remediation.

Network Management: AC-17, Remote Access; AC-18, Wireless Access; CA-7, Continuous Monitoring; CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-4, Security Impact Analysis; CM-6, Configuration Settings; CM-8, Information System Component Inventory; SC-2, Application Partitioning; SC-5, Denial of Service Protection; SC-7, Boundary Protection; SC-10, Network Disconnect; SC-32, Information System Partitioning; and SI-4, Information System Monitoring.

Software Configuration Management: CM-8, Information System Component Inventory; and SA-6, Software Usage Restrictions.

Access Information Management: AC-17, Remote Access; CA-3, Information System Connections; CA-7, Continuous Monitoring; CM-7, Least Functionality; SC-9, Transmission Confidentiality; and SI-12, Information Output Handling and Retention.

Software Assurance: SA-4, Acquisitions; SA-8, Security Engineering Principles; SA-11, Developer Security Testing; SA-12, Supply Chain Protection; SA-13, Trustworthiness; SA-14, Critical Information System Components; and SI-13, Predictable Failure Prevention.

[Source: NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September, 2011.]

The Smart Grid Maturity Model (SGMM)

The Smart Grid maturity model (SGMM)² was initially developed by electric power utilities and is now maintained by the Carnegie Mellon University Software Engineering Institute (SEI). As stated in the SGMM definition document, “The model provides a framework for understanding the current state of Smart Grid deployment and capability within an electric utility and provides a context for establishing future strategies and work plans as they pertain to Smart Grid implementations.” Even though the model is focused on the Smart Grid, its fundamental principles and concepts are applicable and extendable to automation systems.

The SEI provides a suite of SGMM product components to support the model

as follows:

1. Smart Grid Maturity Model Definition – The formal description of the model that includes an overview of the model architecture and is the basis for the other product suite elements.
2. Smart Grid Maturity Model Matrix – A summary of the expected characteristics contained in the model in a tabular format.
3. Smart Grid Maturity Model Compass Assessment – Survey for completion by or on behalf of utilities. Compass questions are designed to collect demographic and performance data and to characterize the status of the responding utility's Smart Grid implementation in the context of the SGMM.
4. Smart Grid Maturity Model Navigator Process – Process developed to help organizations chart a technical, organizational, and operational path through their grid modernization effort.
5. Smart Grid Maturity Model Training – Two courses that support the transition and use of the SGMM.

The scope of the SGMM is illustrated in [Figure 8-7](#):

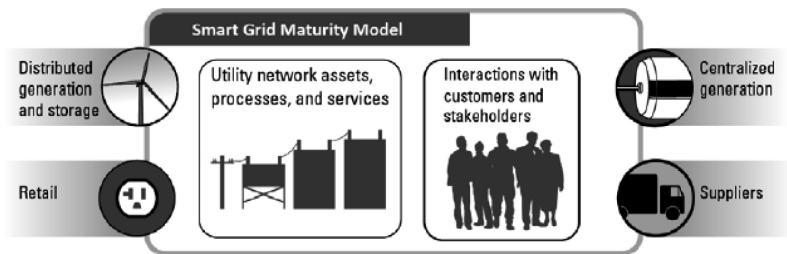


Figure 8-7. The scope of the SGMM

[Source: The Smart Grid Maturity Model, *SGMM Model Definition, A framework for Smart Grid transformation*, Technical Report CMU/SEI-2011-TR-025, Version 1.2, September 2011.]

The model comprises eight domains with each domain having six defined levels of maturity, ranging from Level 0 (lowest) to Level 5 (highest). The model defines a domain as “a logical grouping of Smart Grid characteristics” with each characteristic comprising “a concise, declarative statement to support the consistent evaluation of its implementation and its independence from other characteristics at the same level within the model. The model also requires that for a given level of maturity to be achieved, the expected characteristics for that level and all lower levels in that domain must be

sufficiently implemented.” The eight domains of the SGMM are listed as follows:

- 1.**Strategy, Management, and Regulatory (SMR)** – Represents the capabilities and characteristics that enable an organization to successfully develop a Smart Grid vision and strategy, establish internal governance and management processes, and promote collaborative relationships with stakeholders to implement that strategy and vision.
- 2.**Organization and Structure (OS)** – Represents the organizational capabilities and characteristics that enable an organization to align and operate as required to achieve its desired Smart Grid transformation.
- 3.**Grid Operations (GO)** – Represents the organizational capabilities and characteristics that support the reliable, secure, safe, and efficient operation of the electrical grid.
- 4.**Work and Asset Management (WAM)** – Represents the organizational capabilities and characteristics that support the optimal management of assets and workforce resources (i.e., people and equipment) that are central to meeting Smart Grid goals.
- 5.**Technology (TECH)** – Represents the organizational capabilities and characteristics that enable effective strategic technology planning for Smart Grid capabilities and the establishment of rigorous engineering and business processes for the evaluation, acquisition, integration, and testing of new Smart Grid technology.
- 6.**Customer (CUST)** – Represents the organizational capabilities and characteristics that enable customer participation toward achieving the benefits of the Smart Grid transformation.
- 7.**Value Chain Integration (VCI)** – Represents the organizational capabilities and characteristics that underlie an electric utility’s ability to achieve its Smart Grid goals by successfully managing the utility’s organizational interdependencies with both the supply chain for the production of electricity and the demand chain for its delivery.
- 8.**Societal and Environmental (SE)** – Represents the organizational capabilities and characteristics that enable an organization to contribute to achieving societal goals regarding the reliability, safety, and security of our electric power infrastructure, the quantity and sources of the energy we use, and the impact of the infrastructure and our energy

use on the environment and our quality of life.

An SGMM compass assessment provides an organization with a maturity rating for each of the model's eight domains. The model states that "the six levels of maturity represent defined stages of an organization's progress toward achieving its Smart Grid vision in terms of automation, efficiency, reliability, energy and cost savings, integration of alternative energy sources, improved customer interaction, and access to new business opportunities and markets." The maturity levels are hierarchical in that an organization must reach a Level 1 before progressing to the next levels in sequence. The levels of maturity within each domain are described by a group of expected characteristics and a group of optional informative characteristics.

Expected characteristics are defined as "the capabilities and characteristics that an organization must implement or exhibit to achieve the corresponding maturity level within a domain. Each expected characteristic is presented as a concise, declarative statement to support the consistent evaluation of its implementation and its independence from other characteristics at the same level within the model." Informative characteristics give an additional perspective that provides information concerning whether an organization has achieved a given level of maturity within a domain.

The six maturity levels defined in the SGMM, which are stages of an organization's progress toward achieving its Smart Grid vision, are summarized in [Figure 8-8](#).

The characteristics of each maturity level are summarized as follows:

- Level 0: Default** – The default or entry level of the model across the eight domains of utility. This level precedes an organization's taking significant initial steps toward the adoption of Smart Grid technology.
- Level 1: Initiating** – This level denotes that an organization is taking the first implementation steps toward a Smart Grid within a domain.
- Level 2: Enabling** – Level 2 focuses on implementing features that will enable an organization to achieve and sustain grid modernization.
- Level 3: Integrating** – Level 3 Smart Grid deployments are being integrated across the organization.
- Level 4: Optimizing** – At Level 4, Smart Grid implementations within a given domain are being fine-tuned and used to further increase organizational performance.

•**Level 5: Pioneering** – Organizations at Level 5 are achieving new results with a given domain and advancing the state of the practice.

5	PIONEERING	Organization is breaking new ground and advancing the state of the practice within a domain
4	OPTIMIZING	Organization's smart grid implementation within a given domain is being tuned and used to further increase organizational performance
3	INTEGRATING	Organization's smart grid deployment within a given domain is being integrated across the organization
2	ENABLING	Organization is implementing features within a domain that will enable it to achieve and sustain grid modernization
1	INITIATING	Organization is taking the first implementation steps within a domain
0	DEFAULT	Default level for the model

Figure 8-8. The SGMM maturity levels

[Source: The Smart Grid Maturity Model, *SGMM Model Definition, A framework for Smart Grid transformation*, Technical Report CMU/SEI-2011-TR-025, Version 1.2, September 2011.]

The maturity rating for each domain in an organization is determined by the SGMM Compass survey, which comprises both domain-specific and organizational attribute questions. A typical domain maturity profile determined by a SGMM assessment is shown in [Figure 8-9](#).

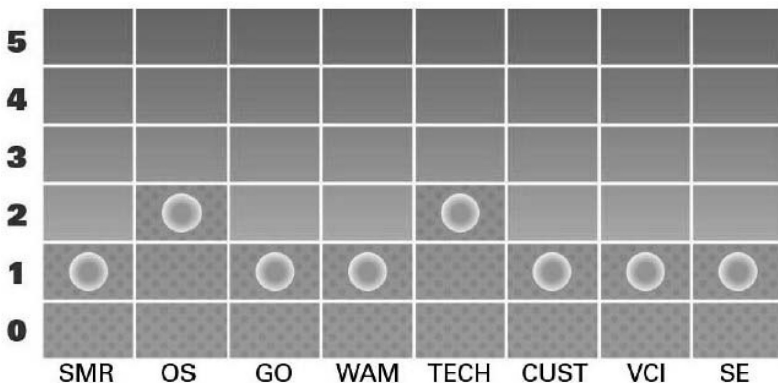


Figure 8-9. Typical SGMM maturity profile

The Smart Grid Maturity Model Matrix

The SGMM Matrix document provides a tabular instantiation of the SGMM model for easy reference. It is presented in [Table 8-2](#).

Automation Maturity Model

In a publication⁶ by the California-Nevada Section of the American Water Works Association (AWWA), Philip Gaberdiel⁶ of Westin Engineering proposed an Automation Maturity Model (AMM) to measure the capability of an organization's industrial automation and control system. The capability implies an increasing level of automation system security, also. The model defines the following six maturity levels of an automation system:

- Level 0 – Local hardwired control
- Level 1 – Local digital control
- Level 2 – Remote manual control
- Level 3 – Remote auto control
- Level 4 – Enhanced operations
- Level 5 – Optimized operations

Table 8-2. SGMM Model Matrix

	Strategy, Management, and Regulatory (SMR) vision, planning, governance, stakeholder collaboration	Organization and Structure (OS) culture, structure, training, communications, knowledge management
PIONEERING 5	1 Smart grid strategy capitalizes on smart grid as a foundation for the introduction of new services and product offerings. 2 Smart grid business activities provide sufficient financial resources to enable continued investment in smart grid sustainment and expansion. 3 New business model opportunities emerge as a result of smart grid capabilities and are implemented.	1 The organizational structure enables collaboration with other grid stakeholders to optimize overall grid operation and health. 2 The organization is able to readily adapt to support new ventures, products, and services that emerge as a result of smart grid. 3 Channels are in place to harvest ideas, develop them, and reward those who help shape future advances in process, workforce competencies, and technology.
OPTIMIZING 4	1 Smart grid vision and strategy drive the organization's strategy and direction. 2 Smart grid is a core competency throughout the organization. 3 Smart grid strategy is shared and revised collaboratively with external stakeholders.	1 Management systems and organizational structure are capable of taking advantage of the increased visibility and control provided by smart grid. 2 There is end-to-end grid observability that can be leveraged by internal and external stakeholders. 3 Decision making occurs at the closest point of need as a result of an efficient organizational structure and the increased availability of information due to smart grid.
INTEGRATING 3	1 The smart grid vision, strategy, and business case are incorporated into the vision and strategy. 2 A smart grid governance model is established. 3 Smart grid leaders with explicit authority across functions and lines of business are designated to ensure effective implementation of the smart grid strategy. 4 Required authorizations for smart grid investments have been secured.	1 The smart grid vision and strategy are driving organizational change. 2 Smart grid measures are incorporated into the measurement system. 3 Performance and/or compensation are linked to smart grid success. 4 Leadership is consistent in communication and actions regarding smart grid. 5 A matrix or overlay structure to support smart grid activities is in place. 6 Education and training are aligned to exploit smart grid capabilities.
ENABLING 2	1 An initial smart grid strategy and a business plan are approved by management. 2 A common smart grid vision is accepted across the organization. 3 Operational investment is explicitly aligned to the smart grid strategy. 4 Budgets are established specifically for funding the implementation of the smart grid vision. 5 There is collaboration with regulators and other stakeholders regarding implementation of the smart grid vision and strategy. 6 There is support and funding for conducting proof-of-concept projects to evaluate feasibility and alignment.	1 A new vision for a smart grid begins to drive change and affect related priorities. 2 Most operations have been aligned around end-to-end processes. 3 Smart grid implementation and deployment teams include participants from all impacted functions and LOBs. 4 Education and training to develop smart grid competencies have been identified and are available. 5 The linking of performance and/or compensation plans to achieve smart grid milestones is in progress.
INITIATING 1	1 Smart grid vision is developed with a goal of operational improvement. 2 Experimental implementations of smart grid concepts are supported. 3 Discussions have been held with regulators about the organization's smart grid vision.	1 The organization has articulated its need to build smart grid competencies in its workforce. 2 Leadership has demonstrated a commitment to change the organization in support of achieving smart grid. 3 Smart grid awareness efforts to inform the workforce of smart grid activities have been initiated.
DEFAULT 0		

	Grid Operations (GO) reliability, efficiency, security, safety, observability, control	Work and Asset Management (WAM) asset monitoring, tracking and maintenance, mobile workforce
PIONEERING 5	1 Self-healing capabilities are present. 2 System-wide, analytics-based, and automated grid decision making is in place.	1 The use of assets between and across supply chain participants is optimized with processes defined and executed across the supply chain. 2 Assets are leveraged to maximize utilization, including just-in-time asset retirement, based on smart grid data and systems.
OPTIMIZING 4	1 Operational data from smart grid deployments is being used to optimize processes across the organization. 2 Grid operational management is based on near real-time data. 3 Operational forecasts are based on data gathered through smart grid. 4 Grid operations information has been made available across functions and LOBs. 5 There is automated decision-making within protection schemes that is based on wide-area monitoring.	1 A complete view of assets based on status, connectivity, and proximity is available to the organization. 2 Asset models are based on real performance and monitoring data. 3 Performance and usage of assets is optimized across the asset fleet and across asset classes. 4 Service life for key grid components is managed through condition-based and predictive maintenance, and is based on real and current asset data.
INTEGRATING 3	1 Smart grid information is available across systems and organizational functions. 2 Control analytics have been implemented and are used to improve cross-LOB decision-making. 3 Grid operations planning is now fact-based using grid data made available by smart grid capabilities. 4 Smart meters are important grid management sensors. 5 Grid data is used by an organization's security functions. 6 There is automated decision-making within protection schemes.	1 Performance, trend analysis, and event audit data are available for components of the organization's systems. 2 CBM programs for key components are in place. 3 Remote asset monitoring capabilities are integrated with asset management. 4 Integration of remote asset monitoring with mobile workforce systems, in order to automate work order creation, is underway. 5 An integrated view of GIS and asset monitoring is in place. 6 Asset inventory is being tracked using automation. 7 Modeling of asset investments for key components is underway.
ENABLING 2	1 Distribution substations are automated and linked to some form of remote distribution automation. 2 Advanced outage restoration schemes are being implemented, which resolve or reduce the magnitude of unplanned outages. 3 Aside from SCADA, piloting of remote asset monitoring of key grid assets to support manual decision making is underway. 4 Investment in and expansion of data communications networks in support of grid operations is underway.	1 An approach to track, inventory, and maintain event histories of assets is in development. 2 An integrated view of GIS for asset monitoring based on location, status, and interconnectivity (nodal) has been developed. 3 An organization-wide mobile workforce strategy is in development.
INITIATING 1	1 Business cases for new equipment and systems related to smart grid are approved. 2 New sensors, switches, and communications technologies are evaluated for grid monitoring and control. 3 Proof-of-concept projects and component testing for grid monitoring and control are underway. 4 Outage and distribution management systems linked to substation automation are being explored and evaluated. 5 Safety and security (physical and cyber) requirements are considered.	1 Enhancements to work and asset management have been built into approved business cases. 2 Potential uses of remote asset monitoring are being evaluated. 3 Asset and workforce management equipment and systems are being evaluated for their potential alignment to the smart grid vision.
DEFAULT 0		

	Technology (TECH) IT architecture, standards, infrastructure, integration, tools	Customer (CUST) pricing, customer participation and experience, advanced services
PIONEERING 5	1 Autonomic computing and machine learning are implemented. 2 The enterprise information infrastructure can automatically identify, mitigate, and recover from cyber incidents.	1 Customers can manage their end-to-end energy supply and usage levels. 2 There is automatic outage detection at the premise or device level. 3 Plug-and-play, customer-based generation is supported. 4 Security and privacy for all customer data is assured. 5 The organization plays a leadership role in industry-wide information sharing and standards development efforts for smart grid.
OPTIMIZING 4	1 Data flows end to end from customer to generation. 2 Business processes are optimized by leveraging the enterprise IT architecture. 3 Systems have sufficient wide-area situational awareness to enable real-time monitoring and control for complex events. 4 Predictive modeling and near real-time simulation are used to optimize support processes. 5 Performance is improved through sophisticated systems that are informed by smart grid data. 6 Security strategy and tactics continually evolve based on changes in the operational environment and lessons learned.	1 Support is provided to customers to help analyze and compare usage against all available pricing programs. 2 There is outage detection and proactive notification at the circuit level. 3 Customers have access to near real-time data on their own usage. 4 Residential customers participate in demand response and/or utility-managed remote load control programs. 5 Automatic response to pricing signals for devices within the customer's premise is supported. 6 In-home net billing programs are enabled. 7 A common customer experience has been integrated.
INTEGRATING 3	1 Smart grid-impacted business processes are aligned with the enterprise IT architecture across LOBs. 2 Systems adhere to an enterprise IT architectural framework for smart grid. 3 Smart grid-specific technology has been implemented to improve cross-LOB performance. 4 The use of advanced distributed intelligence and analytical capabilities are enabled through smart grid technology. 5 The organization has an advanced sensor plan. 6 A detailed data communication strategy and corresponding tactics that cross functions and LOBs are in place.	1 The organization tailors programs to customer segments. 2 Two-way meter communication has been deployed. 3 A remote connect/disconnect capability is deployed. 4 Demand response and/or remote load control is available to residential customers. 5 There is automatic outage detection at the substation level. 6 Residential customers have on-demand access to daily usage data. 7 A common experience has been implemented across two or more customer interface channels. 8 Customer education on how to use smart grid services to curtail peak usage is provided. 9 All customer products and services have built-in standards based on security and privacy controls.
ENABLING 2	1 Tactical IT investments are aligned to an enterprise IT architecture within an LOB. 2 Changes to the enterprise IT architecture that enable smart grid are being deployed. 3 Standards are selected to support the smart grid strategy within the enterprise IT architecture. 4 A common technology evaluation and selection process is applied for all smart grid activities. 5 There is a data communications strategy for the grid. 6 Pilots based on connectivity to distributed IEDs are underway. 7 Security is built into all smart grid initiatives from the outset.	1 Pilots of remote AMI/AMR are being conducted or have been deployed. 2 The organization has frequent (more than monthly) knowledge of residential customer usage. 3 The organization is modeling the reliability of grid equipment. 4 Remote connect/disconnect is being piloted for residential customers. 5 The impact on the customer of new services and delivery processes is being assessed. 6 Security and privacy requirements for customer protection are specified for smart grid-related pilot projects and RFPs.
INITIATING 1	1 An enterprise IT architecture exists or is under development. 2 Existing or proposed IT architectures have been evaluated for quality attributes that support smart grid applications. 3 A change control process is used for applications and IT infrastructure. 4 Opportunities are identified to use technology to improve departmental performance. 5 There is a process to evaluate and select technologies in alignment with smart grid vision and strategies.	1 Research is being conducted on how to use smart grid technologies to enhance the customer's experience, benefits, and participation. 2 Security and privacy implications of smart grid are being investigated. 3 A vision of the future grid is being communicated to customers. 4 The utility consults with public utility commissions and/or other government organizations concerning the impact on customers.
DEFAULT 0		

	Value Chain Integration (VCI) demand and supply management, leveraging market opportunities	Societal and Environmental (SE) responsibility, sustainability, critical infrastructure, efficiency
PIONEERING 5	1 The optimization of energy assets is automated across the full value chain. 2 Resources are adequately dispatchable and controllable so that the organization can take advantage of granular market options. 3 Automated control and resource optimization schemes consider and support regional and/or national grid optimization.	1 Triple bottom line goals align with local, regional, and national objectives. 2 Customers control their energy-based environmental footprints through automatic optimization of their end-to-end energy supply and usage level (energy source and mix). 3 The organization is a leader in developing and promoting industry-wide resilience best practices and/or technologies for protection of the national critical infrastructure.
OPTIMIZING 4	1 Energy resources (including Volt/VAR, DG, and DR) are dispatchable and tradable. 2 Portfolio optimization models that encompass available resources and real-time markets are implemented. 3 Secure two-way communications with Home Area Networks (HANs) are available. 4 Visibility and potential control of customers' large-demand appliances to balance demand and supply is available.	1 The organization collaborates with external stakeholders to address environmental and societal issues. 2 A public environmental and societal scorecard is maintained. 3 Programs are in place to shave peak demand. 4 End-user energy usage and devices are actively managed through the utility's network. 5 The organization fulfills its critical infrastructure assurance goals for resilience, and contributes to those of the region and the nation.
INTEGRATING 3	1 An integrated resource plan is in place and includes new targeted resources and technologies. 2 Customer premise energy management solutions with market and usage information are enabled. 3 Additional resources are available and deployed to provide substitutes for market products to support reliability or other objectives. 4 Security management and monitoring processes are deployed to protect the interactions with an expanded portfolio of value chain partners.	1 Performance of societal and environmental programs are measured and effectiveness is demonstrated. 2 Segmented and tailored information that includes environmental and societal benefits and costs is available to customers. 3 Programs to encourage off-peak usage by customers are in place. 4 The organization regularly reports on the societal and environmental impacts of its smart grid programs and technologies.
ENABLING 2	1 Support is provided for energy management systems for residential customers. 2 The value chain has been redefined based on its smart grid capabilities. 3 Pilots to support a diverse resource portfolio have been conducted. 4 Secure interactions have been piloted with an expanded portfolio of value chain partners.	1 Smart-grid strategies and work plans address societal and environmental issues. 2 Energy efficiency programs for customers have been established. 3 The organization considers a "triple bottom line" view when making decisions. 4 Environmental proof-of-concept projects are underway that demonstrate smart grid benefits. 5 Increasingly granular and more frequent consumption information is available to customers.
INITIATING 1	1 Assets and programs necessary to facilitate load management are identified. 2 Distributed generation sources and the capabilities needed to support them are identified. 3 Energy storage options and the capabilities needed to support them are identified. 4 There is a strategy for creating and managing a diverse resource portfolio. 5 Security requirements to enable interaction with an expanded portfolio of value chain partners have been identified.	1 The smart grid strategy addresses the organization's role in societal and environmental issues. 2 The environmental benefits of the smart grid vision and strategy are publicly promoted. 3 Environmental compliance performance records are available for public inspection. 4 The smart grid vision or strategy specifies the organization's role in protecting the nation's critical infrastructure.
DEFAULT 0		

[Source: The Smart Grid Maturity Model, *Model Matrix Document*, 2011.]

The Automation Maturity Model is illustrated in [Figure 8-10](#).

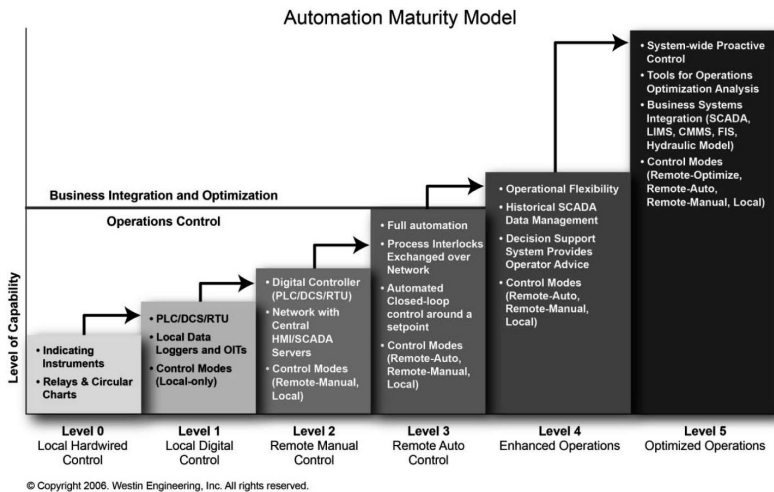


Figure 8-10. The Automation Maturity Model (AMM)

[Source: Phil Gaberdiel, Westin Engineering]

In the model, an automation system at Level 0 is based on relays and instruments read locally, comprising hardware control. Level 1 describes an automation system with local digital control, using PLCs, RTUs, and data loggers, while Level 2 comprises digital controllers and networked HMI/SCADA servers providing remote manual control. A Level 3 remote auto control system includes full automation with automated closed loop controls. Level 4, enhanced operations, has characteristics of operational flexibility, application of decision support systems, and historical SCADA data management. Level 5 achieves optimized operation through the use of operations optimization analysis tools, business systems integration, and systems-wide, proactive control.

Future Smart Grid Issues and Automation Security Issues

Because of the increased number of computational components and sensors that are associated with manufacturing systems, processing plants, and the Smart Grid, the electromagnetic environment will be of increased concern in the future. Even though the following material provides examples relating to the Smart Grid, the issues and countermeasures apply equally to automation systems.

In addition government/industry initiatives such as NIST 7628 are emerging

to address future specific Smart Grid cybersecurity and privacy issues. These two areas are explored in the following sections.

Smart Grid Electromagnetic Radiation Issues

As discussed in [Chapter 5](#), electromagnetic fields have the potential of causing serious interruptions and malfunctions not only in substations, but in “green” energy sources and production facilities. Additional interference that can affect sensitive instrumentation and home-based devices will be present from the increased number of transmitting stations.

In a paper titled *High Power Electromagnetic (HPEM) Threats to the Smart Grid* [3](#), William Radasky describes ongoing efforts to understand and mitigate the effects of electromagnetic radiation on future instantiations of the Smart Grid. Toward this end, an Electromagnetic Interoperability Issues Working Group (EMIIWG) was formed in 2010. The EMIWG is a subgroup of the Smart Grid Interoperability Panel (SGIP), which was established to investigate the interoperability among interconnected components of the Smart Grid. The paper describes the scope of the EMIWG as addressing the following issues:

- Enhancing the immunity of Smart Grid devices and systems to the detrimental effects of natural and man-made electromagnetic interference, both radiated and conducted.
- Developing recommendations for the application of standards and testing criteria to ensure electromagnetic compatibility (EMC) for the Smart Grid, with a particular focus on issues directly related to interoperability of Smart Grid devices and systems.
- Determining impacts, avoidance, generation and mitigation of and immunity to electromagnetic interference.

Specific tasks of the EMIWG associated with these areas of concern include:

- 1.Review potential electromagnetic issues and the existing state of EMC of the power grid and associated systems, including current and proposed Smart Grid enhancements.
- 2.Segment the Smart Grid devices and systems and electromagnetic environments into a minimal set of categories for which electromagnetic issues and EMC requirements can be identified. These categories should be compatible with the environment classifications of IEC 61000-2-5⁴, where possible.
- 3.Prioritize or rank the categories in (2) according to the potential impact on Smart Grid reliability. The priorities should consider the extent and severity of possible failures and the availability requirements for the relevant interface as

defined in NISTIR 7628⁵ (see discussion of NIST 7628 in next section).

4. Identify and/or propose EMC terminology and definitions applicable to the Smart Grid and compatible with international standards.
5. Identify and compile the source-victim matrix for each category identified in (2).
6. Identify or develop EMC performance metrics for systems in each category identified in (2).
7. Identify appropriate EMC standards and requirements to meet performance metrics.
8. Identify areas where EMC standards are not available and identify appropriate standards development organizations (SDO)s where such standards should be developed.
9. Identify and propose priority action plans to address standards or guidelines in high-priority categories if needed.
10. Propose strategic recommendations for EMC of Smart Grid systems, beginning with the highest priority categories. These recommendations should reflect a long-term strategy to maintain EMC as the Smart Grid evolves.
11. Consider the need, and if appropriate, the nature of a conformity assessment program for EMC for coordination with the SGIP Smart Grid Testing and Certification Committee.

A critical task in the above list is task 2, which is basic to the determination of the appropriate EM environment for Smart Grid equipment, which is supported by IEC 61000-2-5. The paper *High Power Electromagnetic (HPEM) Threats to the Smart Grid*, describes the process steps of IEC 61000-2-5 as the following:

1. Define the location classes with regard to the types of exposures (both conducted and radiated) and the distances expected from particular types of emitters.
2. Compile a comprehensive list of radiated and conducted phenomena and disturbance levels along with formulas to compute field levels where appropriate (include formulas for near-field exposure).
3. Combine the results to develop recommendations for disturbance levels for a given “location” for all applicable phenomena.

Related and important guidance documents that will affect the future characteristics of the Smart Grid as well as industrial control systems are NIST Interagency or Internal Reports (NISTIRs), particularly those of NISTIR 7628, cited earlier in this chapter.

NIST 7628

NIST 7628, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cybersecurity*, is a three-volume document that provides a methodical approach to implementing customized cybersecurity and privacy protection strategies for Smart Grid implementations. It was developed by the Cybersecurity Working Group of the Smart Grid Interoperability Panel and is designed to apply to a variety of Smart Grid-related domains, such as electric vehicle charging stations, utilities, manufacturers, and providers of energy management services. Its approach is also directly applicable to process plants, manufacturing operations, and automation systems, in general. It brings together techniques from information system security, information technology, control systems, telecommunications, and manufacturing.

Volume 1 of NIST 7628 addresses the following topics:

- Risk assessment processes to identify high-level security requirements
- High-level architectures
- Logical interface architectures used to identify and define categories of interfaces within and across the Smart Grid domains
- High-level security requirements for the logical interface categories
- Technical cryptographic and key management issues across the scope of Smart Grid systems and devices

Volume II deals with privacy issues in homes and electric vehicles, including:

- Evolving Smart Grid technologies and their relationships with individuals
- Behaviors of groups of individuals and individuals in their dwellings
- Behaviors of groups of individuals and individuals in electric vehicles
- Privacy issues affecting individuals in their premises and electric vehicles

- Recommended privacy practices for participants within the Smart Grid
- Recommendations to consumers involving Smart Grid privacy issues and associated mitigation approaches

Volume III of NIST 7628 is an examination of Smart Grid high-level security requirements, such as:

- Vulnerability categories
- Research and development topics focused on achieving increased security and resilience characteristics for the Smart Grid
- Description of the Cybersecurity Working Group (CSWG) effort to support the evaluation of proposed standards relative to the security needs developed in NIST 7628

Summary

The future environment of industrial automation and control systems will be affected by advances in a number of related and seemingly unrelated fields. Breakthroughs in physics, semiconductors, software engineering, artificial intelligence, communications, information technology, and so on will translate into opportunities and challenges in automation and control systems. No longer can technical personnel rely on narrow control disciplines and ignore the wider technological community if they want to take advantage of progress in those arenas.

In this book, a number of proven, effective techniques have been presented and explored with the goal of providing the management and technical personnel associated with industrial automation and control systems the background and tools to significantly affect the security of our critical automation systems. These methodologies must be embraced and coupled with the latest technological knowledge in order to maximize the security and efficiency of tomorrow's automation and control systems.

Review Questions for Chapter 8

- 1.The technology that eliminates the binding of software to specific hardware platforms is known as which of the following?
 - a.Artificial intelligence

- b.Virtualization
- c.Cloud computing
- d.Software as a service

2.A hypervisor is which of the following?

- a.A virtual machine monitor
- b.An advanced HMI
- c.A manager
- d.An alarm mechanism

3.NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, defines the process for developing an ISCM strategy and implementing an ISCM program. Which one of the following best describes the ISCM strategy?

- a.Providing security mechanisms to reduce risks to automation systems
- b.Developing security policies to specify management intent for information systems and automation systems
- c.Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions
- d.Maintaining ongoing awareness of risk mitigation alternatives

4.Which of the following is NOT one of the ISCM program steps?

- a.Define
- b.Establish
- c.Respond
- d.Mitigate

5.In the ISCM process, the status of automation security in a facility can be determined by establishing appropriate metrics. Which of the following activities is NOT used to define the metrics?

- a.Evaluating applicable mitigation approaches
- b.Assessing all security controls

- c. Providing actionable communication of security status across all tiers of the organization
- d. Collecting, correlating, and analyzing security-related information

6. NIST SP 800-137 defines the process for managing information security and information system–related risk as which of the following?

- a. Risk Management Framework (RMF)
- b. Risk-Impact Criteria (RIC)
- c. Vulnerability Analysis (VA)
- d. Risk-Vulnerability Matrix (RVM)

7. Security control volatility, system categorizations/impact levels, organizational risk tolerance, and security controls with identified weaknesses are associated with what characteristic discussed in NIST 800-137?

- a. The necessity of adding compensating controls
- b. The risk impact levels
- c. The level of risk
- d. The frequency of monitoring security controls for effectiveness

8. Appendix D of NIST SP 800-137 defines a term as “an information security area that includes a grouping of tools, technologies, and data.” What is this term?

- a. Security automation domain
- b. Compensating domain
- c. Risk management domain
- d. Risk mitigation domain

9. The SEI-maintained Smart Grid Maturity Model (SGMM) is described best by which of the following statements?

- a. Provides a framework for understanding the current state of Smart Grid deployment and capability within an electric utility and provides a context for establishing future strategies and work plans as they pertain to Smart Grid implementations

- b. Provides a management perspective of Smart Grid deployment and capability within an electric utility and develops guidelines for Smart Grid implementations
- c. Provides a targeted hierarchical methodology applicable to Smart Grid evaluation and maintenance within an electric utility and provides a basis for implementing effective Smart Grid controls
- d. Provides a Smart Grid assurance model and algorithms for future deployment and implementation of Smart Grid systems

10. Which of the following is NOT one of the eight domains of the SGMM?

- a. Strategy, Management, and Regulatory (SMR)
- b. Organization and Structure (OS)
- c. Metering and Monitoring (MAM)
- d. Work and Asset Management (WAM)

11. Which of the following is NOT one of the six maturity levels defined in the SGMM?

- a. Default
- b. Evaluating
- c. Initiating
- d. Integrating

12. The SGMM maturity rating for each domain in an organization is determined by which of the following means?

- a. The SGMM Domain survey
- b. The SGMM Risk survey
- c. The SGMM Level survey
- d. The SGMM Compass survey

13. NIST 7628, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cybersecurity*, is a three-volume document that provides a methodical approach to implementing customized cybersecurity and privacy protection strategies for Smart Grid implementations. Which of the following areas is NOT addressed in the volumes comprising NISTIR 7628?

- a.Risk assessment processes
- b.Privacy issues
- c.Cost evaluation matrices
- d.Research and development topics

14.Which of the following describes the optimizing level (Level 4) of the SGMM?

- a.Focuses on implementing features that will enable an organization to achieve and sustain grid modernization
- b.Smart Grid implementations within a given domain are being fine-tuned and used to further increase organizational performance
- c.Smart Grid deployments are being integrated across the organization
- d.Organizations are achieving new results with a given domain and advancing the state of the practice

15.What entity in the SGMM is defined as “the stages of an organization’s progress toward achieving its Smart Grid vision in terms of automation, efficiency, reliability, energy and cost savings, integration of alternative energy sources, improved customer interaction, and access to new business opportunities and markets?”

- a.Maturity
- b.Capability
- c.Characteristics
- d.Value

16.In the ISCM process, the status of automation security in a facility can be determined by establishing appropriate metrics. The metrics are defined through the following activities, except one, which is not applicable. Which of the following is NOT applicable?

- a.Maintaining an understanding of threats and threat activities
- b.Conducting security awareness training
- c.Collecting, correlating, and analyzing security-related information
- d.Active management of risk by organizational officials

17. What technology reduces the effort required to maintain hardware and software systems by eliminating the binding of software to specific hardware platforms through the logical partitioning of physical computing resources into multiple execution environments, including servers, applications, and operating systems?
- a. Virtualization
 - b. Cloud computing
 - c. Distributed computing
 - d. Multi-core chips
18. Which of the following statements is FALSE regarding penetration testing of industrial automation and control systems?
- a. If not properly conducted, penetration testing can cause damage to automation systems and disrupt operations.
 - b. Penetration testing tools do not create additional traffic on automation networks and do not affect systems with limited memory capacity.
 - c. If executed properly, penetration testing can provide important information regarding the security of automation systems.
 - d. It is useful to use nonintrusive methods when conducting penetration testing.
19. Penetration testing conducted with no prior knowledge of the automation system is known as which of the following?
- a. Black box
 - b. White box
 - c. Grey box
 - d. Auto box
20. Which of the following is NOT a component of the reconnaissance phase of penetration testing?
- a. Footprinting
 - b. Scanning
 - c. Controlling
 - d. Enumerating

21.Which of the following is NOT one of the maturity levels of the Automation Maturity Model?

- a.Local digital control
- b.Remote auto control
- c.Optimized operations
- d.Enabled control

22.What level of the Automation Maturity Model is characterized by full automation and automated closed-loop control around a set point?

- a.Local digital control
- b.Enhanced operations
- c.Remote auto control
- d.Optimized operations

References

- [1](#) NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011.
- [2](#) The Smart Grid Maturity Model, *SGMM Model Definition, A Framework for Smart Grid Transformation*, Technical Report CMU/SEI-2011-TR-025, Version 1.2, September 2011.
- [3](#) Radasky, W. "EMC and the Smart Grid," *Interference Technology 2011*, EMC Test and Design Guide, 2011.
- [4](#) IEC 61000-2-5 Edition 2, *Description and Classification of Electromagnetic Environments*, Geneva: International Electrotechnical Commission, May 2011.
- [5](#) Introduction to NISTIR 7628, *Guidelines for Smart Grid Cybersecurity*, The Smart Grid Interoperability Panel Cybersecurity Working Group, September 2010.
- [6](#) Gaberdiel, P. "Taking Your SCADA System to the Next Level," *SOURCE*, Volume 25, Number 3, CA-NV Section, AWWA, Summer, 2011.

Appendix A

Review Questions and Answers

Review Questions for Chapter 1

(Please read the questions carefully and select the one BEST answer.)

1. According to NIST SP 800-82, the term “industrial control system” encompasses which of the following?

- a. SCADA systems
- b. Distributed control systems (DCSs)
- c. Programmable logic controllers (PLCs)
- d. All of the above

Answer: d

2. According to ANSI/ISA-99.00.01, “a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process” is a(n):

- a. Industrial automation and control system
- b. Distributed control system
- c. Discrete control system
- d. Programmable logic controller

Answer: a

3. A “type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems” is defined by ANSI/ISA-99.00.01 as which of the following?

- a. Distributed control system
- b. SCADA system
- c. Safety instrumented system (SIS)

d.Human-machine interface (HMI)

Answer: b

4.Which one of the following items is NOT a component of a classical SCADA system model?

a.Human-machine interface (HMI)

b.Remote terminal unit (RTU)

c.Enterprise resource planning (ERP)

d.Programmable logic controller (PLC)

Answer: c. ERP is a resource used by management systems.

5.Which of the following is NOT a characteristic of a SCADA master terminal unit (MTU)?

a.Has two-way communication with field devices

b.Usually located at the master control center

c.Has high-bandwidth communication requirements

d.Communicates through telephone, VHF/UHF radio, spread spectrum radio, satellite, and/or microwave

Answer: c. A MTU has low-bandwidth communication requirements.

6.In a typical SCADA application, what component serves as a data concentrator and is an interface between the MTU and field devices?

a.HMI

b.RTU

c.Data historian

d.Relational database

Answer: b

7.IEC standard 61131-3 was designed to make it easier to implement control logic functions. IEC 61131-3 is which of the following?

a.Vendor-independent international standard for PLC programming languages

b.Standard guide to industrial control systems

- c.Safety instrumented systems (SIS) standard for the process industry
- d.Integrated enterprise-wide risk management standard

Answer: a

8.Which of the following is NOT a characteristic of a data historian?

- a.Provides for prompt recovery of data
- b.Performs data compression
- c.Supports interactive storage and retrieval of detailed production information
- d.Provides system histories over given time periods

Answer: c. Interactive storage and retrieval are functions of real-time relational databases.

9.A yield accounting system used in conjunction with a SCADA system provides which of the following functions?

- a.Plant material movement
- b.Inventory discrepancies
- c.Material balances
- d.All of the above

Answer: d

10.ANSI/ISA-99.00.01-2007 defines which of the following as “a type of control system in which the system elements are dispersed but operated in a coupled manner?”

- a.Distributed control system
- b.Discrete control system
- c.Dispersed control system
- d.Coupled control system

Answer: a. Answer b, a discrete control system, is one in which parameters at one or more points may change only at discrete values of time. Answers c and d are made-up distracters.

11.ANSI/ISA-84.00.01-2004 Part 1(IEC 61511-1 Mod) defines which of the following as an “instrumented system used to implement one or more

safety instrumented functions (SIF)”?

- a.Safety surety system
- b.Failure proof system
- c.Safety instrumented system
- d.Safety function system

Answer: c. The other answers are made-up distracters.

12.Necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use is known as which of the following?

- a.Safety duration
- b.Safety life cycle
- c.Safety boundary
- d.Safety period

Answer: b

13.The safety integrity level (SIL) is a discrete level for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Which of the following statements is TRUE?

- a.Safety integrity level 4 has the lowest level of safety integrity; safety integrity level 1 has the highest.
- b.Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.
- c.Safety integrity level 3 has the highest level of safety integrity; safety integrity level 1 has the lowest.
- d.Safety integrity level 3 has the lowest level of safety integrity; safety integrity level 1 has the highest.

Answer: b

14.The Open Systems Interconnection (OSI) reference model has how many layers?

- a.Six
- b.Five

c.Seven

d.Four

Answer: c. The layers are application, presentation, session, transport, network, data link, and physical.

15.Which layer of the OSI model converts packets into electrical or optical signals for sending on the transmission media?

a.Application

b.Presentation

c.Physical

d.Session

Answer: c

16.What are the four layers of the TCP/IP model?

a.Application, Host-to-Host, Internet, and Network Access

b.Application, Presentation, Internet, and Network Access

c.Application, Network, Internet, and Network Access

d.Application, Host-to-Host, Internet, and Physical

Answer: a

17.NIST 800-82 defines which of the following as “a set of open standards developed to promote interoperability between disparate field devices, automation/control, and business systems”?

a.Modbus/TCP

b.OPC

c.DNP3

d.Profibus

Answer: b

18.The protocol that supports the communication of safety-related data over a variety of industrial networks and ensures data transfer integrity is known as which of the following?

a.Safety instrumented system (SIS)

b.Safety instrumented function (SIF)

c.OpenSAFETY

d.ClosedSafety

Answer: c

19.Which of the following statements relative to the IEC layered architecture Standard IEC 61850 for substation automation is NOT true?

a.It is a set of protocols for electric utilities.

b.IEC-enabled devices can obtain power grid condition data via an Ethernet process bus.

c.Merge units provide interfaces to field devices.

d.It is not compatible with legacy protocols.

Answer: d

20.Which of the following are versions of Profibus?

a.Profibus PA, Profibus CP, Profibus CIP

b.Profibus PA, Profibus DP, Profibus FMS

c.Profibus PA, Profibus CP, Profibus FMS

d.Profibus PA, Profibus CIP, Profibus FMS

Answer: b

Review Questions for Chapter 2

1.Information system security is defined as comprising which of the following three basic elements?

a.Confidentiality, integrity, and authorization

b.Confidentiality, integrity, and availability

c.Audit, integrity, and availability

d.Security, integrity, and availability

Answer: b

2.Protecting documents and messages from unauthorized disclosure refers to which of the following?

- a. Confidentiality
- b. Availability
- c. Authorization
- d. Integrity

Answer: a

3. An attack that overloads the resources of a computing system is an attack against which of the following?

- a. Integrity
- b. Availability
- c. Confidentiality
- d. Authentication

Answer: b

4. Which of the following items refers to the act of verifying a user's identity and confirming that a user is who he or she professes to be?

- a. Authentication
- b. Authorization
- c. Registration
- d. Accountability

Answer: a

5. Which of the following is a detective activity used to determine if violations of information system security have occurred?

- a. Confirming
- b. Authenticating
- c. Auditing
- d. Authorizing

Answer: c

6. Ensuring that the sender of a message or contract cannot later deny sending the message or contract is known as which of the following?

- a. Nonrepudiation

- b.Denial
- c.Validation
- d.Confirmation

Answer: a

7.A security control that minimizes the effect of an attack and the degree of resulting damage is known as which type of control?

- a.Corrective
- b.Preventive
- c.Deterrent
- d.Detective

Answer: a

8.The Information Assurance Technical Framework Forum (IATF) Document 3.1 ([Table 2-1](#)) defines which of the following attacks as an “attempt to circumvent or break protection features, introduce malicious code, or steal or modify information”?

- a.Distribution
- b.Close-in
- c.Active
- d.Passive

Answer: c

9.The act of establishing numerous layers of protection wherein a subsequent layer will provide protection if a previous layer is breached is known as which of the following?

- a.Defense in depth
- b.Complete mediation
- c.Least privilege
- d.Open design

Answer: a

10.Which of the following is noncompulsory?

- a.Standards

- b.Guidelines
- c.Policies
- d.Procedures

Answer: b

11.A self-replicating or self-reproducing program that spreads by inserting copies of itself into other executable code or documents is known as which of the following?

- a.Worm
- b.Mobile code
- c.Back door
- d.Virus

Answer: d

12.An attack that focuses on the authentication protocol between a claiming party and a verifying party communicating with each other is known as which of the following?

- a.Meet-in-the-middle
- b.Man-in-the-middle
- c.Social engineering
- d.Brute force

Answer: b

13.NIST SP 800-41 defines which of the following as “devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures”?

- a.Firewalls
- b.Demilitarized zones
- c.Trap doors
- d.Browsers

Answer: a

14.What type of firewall filters packets based on firewall access control lists (ACLs), which specify the packets that can be sent to particular destination addresses, or on specific application port destinations?

- a.Stateful inspection
- b.Packet filtering
- c.Application proxy
- d.Screened-host

Answer: b

15.What type of firewall serves as an intermediary between networks and serves to mask the source of a message?

- a.Application
- b.Packet filtering
- c.Stateful inspection
- d.Application proxy

Answer: d

16.What type of firewall defines a demilitarized zone (DMZ) or perimeter network, which is a third network that lies between the internal trusted network and the external untrusted network as an added layer of protection?

- a.Dual-homed host
- b.Screened-subnet
- c.Screened-host
- d.Application

Answer: b

17.What type of cryptography uses public and private key pairs?

- a.Symmetric
- b.Asymmetric
- c.Secret key
- d.Transposition

Answer: b

18.The Advanced Encryption Standard (AES) is an example of which of the following types of cryptography?

- a.Symmetric key
- b.Asymmetric key
- c.Public key
- d.Dual key

Answer: a

19.The result of a variable length message being fed into a hash function is a shorter, fixed length output digital stream, known as which of the following?

- a.Ciphertext
- b.Plaintext
- c.Message digest
- d.Cryptovvariable

Answer: c

20.A digital signature uses asymmetric key encryption to achieve which of the following?

- a.Nonrepudiation
- b.Nonrepudiation and authentication
- c.Authorization
- d.Confidentiality

Answer: b

21.A cryptographic attack in which the attacker has access to multiple samples of encrypted messages that have been encrypted with the same algorithm and attempts to find the key is known as which of the following?

- a.Chosen ciphertext
- b.Ciphertext only
- c.Adaptive chosen ciphertext
- d.Known plaintext

Answer: b

22.A private network that operates as an overlay on a public infrastructure is

known as which of the following?

- a.Virtual private network
- b.Dual band network
- c.4G network
- d.Demilitarized zone

Answer: a

23.IPsec provides which of the following two modes of operation?

- a.Symmetric key mode and transport mode
- b.Authentication mode and tunnel mode
- c.Transport mode and tunnel mode
- d.Transport mode and transparent mode

Answer: c

24.A VPN that provides secure communications over a public network between two trusted networks is known as which of the following?

- a.Host-to-host
- b.Gateway-to-gateway
- c.Host-to-gateway
- d.Host-to-demilitarized zone

Answer: b

Review Questions for Chapter 3

1.Which of the following statements is generally TRUE regarding an industrial automation and control system?

- a.Installation of software patches can be performed routinely and frequently.
- b.Encryption of data can sometimes lead to problematic delays.
- c.Penetration testing can be conducted routinely and frequently.

d. Confidentiality is a key concern in automation systems as opposed to integrity and availability.

Answer: b

2. In both IT and automation and control systems, which of the following is the primary concern in the event of an emergency or malicious event?

- a. Equipment safety
- b. Preservation of documentation
- c. Personnel safety
- d. Facility protection

Answer: c

3. Which of the following statements is FALSE?

- a. Flash drives and other portable memory devices can be sources of malware injections into control systems.
- b. Maintenance hooks and trap doors installed in automation and control systems for remote maintenance can be easy entry points to modify critical software and firmware with negative consequences.
- c. In many control system environments, control engineers, in general, do not have multiple responsibilities, such that the security principle of separation of duties is not normally violated.
- d. Many facilities house legacy systems with outdated technology, minimal memory and computing power, and little thought to security.

Answer: c

4. Which of the following actions is the most likely to result in blockages and lack of system availability in automation and control systems?

- a. Remote access
- b. Life cycle design
- c. Accountability
- d. Port scanning

Answer: d

5.Which threat source is motivated by revenge, ego, and dissatisfaction?

- a.Insider
- b.Espionage
- c.Criminal
- d.Hacker

Answer: a

6.What is a source of a possible disruption of control system functions that is not normally considered?

- a.Changes from digital to analog systems
- b.Upgrades from analog to digital systems
- c.Malware
- d.Attacks

Answer: b

7.In general, what distinguishes analog control equipment from digital control equipment?

- a.Analog controls generate more high-frequency peak voltages than digital controls.
- b.Digital controls generate more high-frequency peak voltages than analog controls.
- c.Analog controls generate essentially the same number of high-frequency peak voltages as digital controls.
- d.Digital controls generate essentially the same number of high-frequency peak voltages as analog controls.

Answer: b

8.Which of the following is more likely to be performed in an IT environment than in an automation and control system environment?

- a.Security architecture analysis
- b.Information security testing
- c.Quantitative risk analysis
- d.Change management

Answer: d

9. Which of the following is more likely to be a common area of security practice that is equally performed in both IT and automation and control systems?

- a. Information security management
- b. Information processing controls
- c. Email security
- d. Digital signatures

Answer: a

10. Which of the following threat sources is motivated by economic exploitation and competitive advantage, and uses social engineering?

- a. Insider
- b. Terrorist
- c. Industrial espionage
- d. Computer criminal

Answer: c

11. What is a detective control that is more frequently applied in IT systems than in control and automation systems?

- a. Firewall
- b. Separation of duties
- c. Biometrics
- d. Auditing

Answer: d

12. Which of the following is NOT a usual reason for an organization's reluctance to disclose successful attacks against it?

- a. Hope the attack will harm competitors
- b. Embarrassment
- c. Effect on reputation
- d. Possible loss of customers

Answer: a

13.Which of the following can lead to a single point of failure in an industrial automation and control system?

- a.Separation of duties
- b.Disk redundancy
- c.Combination of safety and security mechanisms
- d.Use of authentication with identification

Answer: c

14.What is a typical characteristic of industrial automation and control systems?

- a.Have excess computing cycles
- b.Have limited extra computing cycles
- c.Have excess memory
- d.Computational speed is not an issue

Answer: b

15.What is a typical characteristic of an automation and control system supplier?

- a.Usually ensures maintenance hooks are never left enabled without the customer's approval
- b.Usually ensures default passwords are never duplicated from one customer to another
- c.Usually provides unmodified off-the-shelf hardware and software
- d.Usually provides modified hardware and software

Answer: d

Review Questions for Chapter 4

1.Which of the following is an important element in connecting to smart meters?

- a.Home area network
- b.Energy storage devices

c.Cloud computing

d.Printers

Answer: a

2.Energy storage devices are especially useful in which of the following cases?

a.Fossil fuel energy sources

b.Nonrenewable energy sources

c.Intermittent renewable energy sources

d.Constant energy sources

Answer: c

3.The application of data mining and analysis to large amounts of data for the purposes of discovering knowledge and making intelligent predictions and decisions is known as which of the following?

a.Artificial intelligence

b.Analytics

c.Data aggregation

d.Predictive calculus

Answer: b

4.Which of the following techniques is used for condition monitoring of high voltage electrical equipment and identifying areas of potential failure?

a.Analytics

b.Artificial intelligence

c.Robotics

d.Scanning

Answer: a

5.Data from a variety of sources that is analyzed in real time or near real time to perform predictive modeling and support physical, logical, and administrative security is known as which of the following?

a.Data aggregation

b.Cyber analytics

- c.Cybersecurity
- d.Sensitivity analysis

Answer: b

6.What of the following is NOT a characteristic of cloud computing?

- a.Measured service
- b.Resource pooling
- c.On-demand self-service
- d.Minimal elasticity

Answer: d

7.Which of the flowing is NOT one of the three cloud service models?

- a.Cloud application as a service
- b.Cloud software as a service
- c.Cloud platform as a service
- d.Cloud infrastructure as a service

Answer: a

8.Which of the following is NOT one of the five basic privacy principles?

- a.Access
- b.Choice
- c.Preemption
- d.Notice

Answer: c

9.Which of the following items is NOT one of the European Union (EU) privacy principles?

- a.Data should be collected in accordance with the law.
- b.Data should be used only for the purposes for which it was collected, and it should be used only for a reasonable period of time.
- c.Transmission of personal information to locations where equivalent personal data protection cannot be assured

is permitted.

d. Individuals have the right to correct errors contained in their personal data.

Answer: c

10. The ability of an entity to exchange information with another entity is known as which of the following?

- a. Compatibility
- b. Commonality
- c. Interchangeability
- d. Interoperability

Answer: d

11. Which of the following is NOT a distinguishing characteristic of the Smart Grid?

- a. Development and incorporation of demand response, demand-side resources, and energy efficiency resources
- b. Deployment and integration of distributed resources and generation, excluding renewable resources
- c. Provision to consumers of timely information and control options
- d. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid

Answer: b

12. Which of the following is NOT an expected result of Smart Grid implementation?

- a. Higher grid resiliency
- b. Improved energy delivery efficiency
- c. Reduced operating costs
- d. Possible loss of customers

Answer: d

13.Which of the following is NOT a domain in the NIST Smart Grid framework?

- a.Control
- b.Customer
- c.Operations
- d.Bulk generation

Answer: a

14.Which domain of the Smart Grid framework provides energy generated from sources such as coal, gas, water from dams, nuclear reactions, geothermal, the sun, and wind?

- a.Distribution
- b.Transmission
- c.Bulk generation
- d.Service provider

Answer: c

15.Which domain of the Smart Grid delivers electrical power to the distribution domain and balances the required electrical load?

- a.Transmission
- b.Service provider
- c.Operations
- d.Bulk generation

Answer: a

16.Which domain of the Smart Grid handles customer problems and manages business accounts?

- a.Markets
- b.Service provider
- c.Markets
- d.Operations

Answer: b

17.What subsystem of the Smart Grid comprises hardware and meter data management (MDM) software that provide the normal meter reading functions as well as supporting two-way communications that can exchange energy information and commands with customer's devices through a home area network?

- a.Advanced Metering Infrastructure (AMI)
- b.Energy Management System (EMS)
- c.Energy Services Interface (ESI)
- d.Smart Grid Interface (SGI)

Answer: a

18.In Smart Grid Terminology, DER stands for which of the following terms?

- a.Delayed energy reduction
- b.Determined energy requirements
- c.Distributed energy requirements
- d.Distributed energy resources

Answer: d

19.Which domain of the Smart Grid framework has a home area network and also might have a requirement for energy storage for intermittent sources of electricity?

- a.Customer
- b.Distribution
- c.Operations
- d.Markets

Answer: a

20.Which domain of the Smart Grid framework handles large amounts of customer personally identifiable information and must ensure that adequate privacy protections are in place?

- a.Customer
- b.Markets
- c.Service provider
- d.Operations

Answer: c

21. Which of the following evolving technologies can increase communications, collaboration, and innovation, but also be a source of compromise of PII and other sensitive information?

- a. Social networks
- b. Interoperability
- c. Cloud computing
- d. Analytics

Answer: a

22. Which domain of the Smart Grid framework does not have an energy storage requirement for intermittent sources of electricity?

- a. Customer
- b. Transmission
- c. Bulk generation
- d. Markets

Answer: d

23. Which domain of the Smart Grid framework has the most potential for benefiting from the use of cloud computing?

- a. Customer
- b. Transmission
- c. Distribution
- d. Operations

Answer: d

Review Questions for Chapter 5

1. In ANSI/ISA-99.00.01-2007, a “potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm,” is which of the following?

- a. Threat
- b. Vulnerability
- c. Weakness
- d. Risk

Answer: a

2. The “expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence” is which of the following?

- a. Consequence
- b. Threat source
- c. Weakness
- d. Risk

Answer: d

3. The program and supporting processes to manage information security risk to organizational operations (i.e., mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation are defined as which of the following?

- a. Risk assessment
- b. Risk management
- c. Risk mitigation
- d. Risk association

Answer: b

4. Which of the following is considered an asset in risk management?

- a. Computer hardware

- b.A control system
- c.A professional with unique knowledge
- d.All of the above

Answer: d

5.The ANSI/ISA-99.02.01-2009 Cybersecurity Management System (CSMS) comprises which of the following three main categories?

- a.Risk analysis, addressing the risk, and monitoring and improving the CSMS
- b.Risk mitigation, addressing the risk, and monitoring and improving the CSMS
- c.Risk analysis, addressing the risk, and monitoring and improving the automation system
- d.Risk analysis, eliminating the risk, and monitoring and improving the CSMS

Answer: a

6.In the CSMS, a business rationale is established. Which of the following is NOT one of the elements of the business rationale?

- a.Establishing a basis for securing the industrial automation and control system
- b.Obtaining management support for securing automation systems
- c.Identifying and understanding the consequences of a successful attack on automation systems
- d.Confirmation of the value of the automation system

Answer: d

7.The risk identification, classification, and assessment activities of the CSMS do NOT include which of the following?

- a.Conduct a high-level risk assessment
- b.Develop simple network diagrams
- c.Mitigate the risk
- d.Perform a detailed vulnerability assessment

Answer: c

8.Which of the following is NOT one of the areas included in “Addressing risk with the CSMS?”

- a.Security policy, organization and awareness
- b.Correction
- c.Selected security countermeasures
- d.Implementation

Answer: b

9.Subdividing a network into zones that have similar security requirements and characteristics and are separated by protective devices to screen traffic from one network segment to another is known as which of the following?

- a.Network segmentation
- b.Network isolation
- c.Network masking
- d.Network fragmentation

Answer: a

10.In the CSMS, access control is subdivided into which of the following three areas?

- a.Account verification, authentication, and authorization
- b.Account administration, authentication, and authorization
- c.Account administration, audit, and authorization
- d.Account administration, authentication, and activation

Answer: b

11.Risk management, system development and maintenance, and incident planning are part of which of the following areas of addressing risk in the CSMS?

- a.Security policy, organization, and awareness
- b.Selected security countermeasures
- c.Implementation
- d.Scope

Answer: c

12. In the monitoring and improving category of the CSMS, which element verifies that an automation system is compliant with appropriate policies, procedures, and regulations?

- a. Review
- b. Conformance
- c. Improve
- d. Maintain

Answer: b

13. NIST SP 800-39 views which of the following as a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis?

- a. Risk management
- b. Risk assessment
- c. Risk monitoring
- d. Risk evaluation

Answer: a

14. NIST SP 800-39 defines three tiers. Which of the following include those three?

- a. Policy, Mission/Business Processes, Information Systems
- b. Organization, Policy, Information Systems
- c. Organization, Mission/Business Processes, Objectives
- d. Organization, Mission/Business Processes, Information Systems

Answer: d

15. Categorizing organizational information systems and properly allocating security controls to those systems to support the organization's mission/business processes is performed in which tier of the multitiered risk management architecture?

- a. Tier 1
- b. Tier 2
- c. Tier 3

d.Tier 4

Answer: c

16.According to NIST SP 800-39, risk framing, risk assessment, risk response, and risk monitoring are components of which of the following?

- a.Risk valuation
- b.Risk determination
- c.Risk management
- d.Risk acceptance

Answer: c

17.Making assumptions about threats, vulnerabilities, consequences/impact, and likelihood of occurrence are part of which of the following, according to NIST SP 800-39?

- a.Risk assessment
- b.Risk framing
- c.Risk response
- d.Risk monitoring

Answer: b

18.Which of the following is NOT an element of responding to risk, according to NIST SP 800-39?

- a.Evaluating the effectiveness of implemented risk response measures
- b.Developing alternative courses of action
- c.Selecting the best courses of action
- d.Implementing selected responses

Answer: a

19.According to NIST SP 8000-37, which of the following “provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle?”

- a.Risk Monitoring Framework (RMF)
- b.Risk Assessment Framework (RAF)

c.Risk Management Framework (RMF)

d.Risk Evaluation Framework (REF)

Answer: c

20.Which of the following groups of elements is presented in NIST SP 800-37 to manage risk?

a.Categorize, Select, Implement, Authorize

b.Categorize, Evaluate, Implement, Monitor

c.Determine, Select, Implement, Authorize

d.Determine, Evaluate, Implement, Monitor

Answer: a

21.Which of the following is NOT characteristic of an insider threat?

a.Many insider attacks are conducted by disgruntled insiders

b.Most insider attacks do not result in serious losses or harm

c.Many insider attacks are conducted remotely

d.Many inside attackers have privileged access to computer systems

Answer: b

22.Which of the following best describes Stuxnet?

a.A worm that was designed to change control outputs on specific PLCs and conceal its existence from control room observers

b.A worm that was designed to modify email messages and conceal its existence from control room observers

c.A virus that was designed to modify disk storage and send random messages to users' computers

d.A virus that was designed to crash computers when email attachments were opened

Answer: a

23.Which of the following is NOT true regarding Stuxnet?

a.Attacks both networked and non-networks PCs

- b.Installs device drivers using valid, digital certificates
- c.Infects Apple Macintosh computers
- d.Infection is accomplished through USB flash drives

Answer: c

24.The process that only uses software that is “clean” and not compromised and is verified before running is known as which of the following?

- a.Confirming
- b.Whitelisting
- c.Cleanlisting
- d.Prechecking

Answer: b

25.An electromagnetic pulse generated by a high-altitude nuclear detonation in space at heights above 30 km is known as which of the following?

- a.Intentional Electromagnetic Interference (IEMI)
- b.Space Generated EMP (SGEMP)
- c.Intensive Electromagnetic Interference (IEMI)
- d.High Altitude EMP (HEMP)

Answer: d

26.Which one of the following is NOT a component of a High Power Electromagnetic (HPEM) burst?

- a.Final-time (E4) – Several hundred seconds after the burst
- b.Early-time (E1) – Within 10 ns of the burst
- c.Intermediate-time (E2) – Between 1 microsecond and 1 second after the burst
- d.Late-time (E3) – Between 1 second and several hundred seconds after the burst

Answer: a

27.Solar-generated EMP is the result of which of the following actions?

- a.Changes in the sun’s orbit

- b.Solar eclipses
- c.Geomagnetic storms on the sun
- d.Changes in the earth's orbit

Answer: c

28.Which of the following statements is NOT true regarding EMP?

- a.High-frequency pulses can induce currents in floating wires.
- b.High-frequency pulses can penetrate through windows and gaps in metal shields.
- c.High-frequency grounding with filters and surge arrestors can be used to protect sensors, smart meters, and communications systems.
- d.Fiber optic cabling cannot minimize coupling.

Answer: d

Review Questions for Chapter 6

1.NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, partitions security controls into which one of the following groups?

- a.Management controls, operational controls, and technical controls
- b.Management controls, administrative controls, and technical controls
- c.Management controls, operational controls, and physical controls
- d.Logical controls, operational controls, and technical controls

Answer: a

2.NIST SP 800-82 defines five major security objectives for an industrial control system (ICS) implementation. Which of the following is NOT one of those objectives?

- a.Restricting logical access to the ICS network and network activity

- b.Restricting physical access to the ICS network and devices
- c.Protecting individual ICS components from exploitation
- d.Shutting down the ICS after an incident

Answer: d

3.In NIST SP 800-82, policies and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation is known as which of the following?

- a.Configuration management
- b.Risk management
- c.System management
- d.System maintenance

Answer: a

4.In the NIST SP 800-82 controls, the process of granting or denying specific requests for obtaining and using information and related information processing services for physical access to areas within the information system environment is known as which of the following?

- a.Authentication
- b.Audit and accountability
- c.Access control
- d.Identification

Answer: c

5.The controls of ANSI/ISA-TR99.00.01-2007 are organized into six categories. Which of the following is NOT one of those categories?

- a.Encryption Technologies and Data Validation
- b.Risk Mitigation Technologies
- c.Authentication and Authorization Technologies
- d.Filtering/Blocking/Access Control Technologies

Answer: b

6.ANSI/ISA-TR99.00.01-2007 describes which of the following as “the initial

step in protecting an industrial automation and control system (IACS) and its critical assets from unwanted breaches. It is the process of determining who and what should be allowed into or out of a system”?

- a.Authorization
- b.Authentication
- c.Identification
- d.Confirmation

Answer: a

7.Which of the following are the major components of authentication and authorization technologies spelled out in ANSI/ISA-TR99.00.01-2007?

- a.Role-based, password, and challenge response
- b.Rule-based, user ID, and challenge response
- c.Role-based, password, and call-back
- d.Rule-based, password, and call-back

Answer: a

8.Which of the following does ANSI/ISA-TR99.00.01-2007 identify as the three main types of software that have to be considered in industrial automation and control system software?

- a.Mobile operating systems, real-time and embedded operating systems, and Web servers and Internet technologies
- b.Server and workstation operating systems, real-time and embedded operating systems, and wireless technologies
- c.Server and workstation operating systems, real-time and embedded operating systems, and Web servers and Internet technologies
- d.Server and workstation operating systems, real-time and embedded operating systems, and mobile technologies

Answer: c

9.In ANSI/ISA-TR99.00.01-2007, what are the three main categories of physical security elements?

- a.Active, identification and monitoring devices, and passive

- b.Active, real-time, and passive
- c.Active, identification and monitoring devices, and real-time
- d.Reactive, identification and monitoring devices, and passive

Answer: a

10.The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cybersecurity Standards are divided into Standards CIP-002-4 through CIP-009-4 and address “the identification and protection of critical cyber assets to support reliable operation of the Bulk Electric System (BES).” Which of the following is NOT one of the eight standards?

- a.Risk assessment
- b.Critical cyber asset identification
- c.Security management controls
- d.Electronic security perimeters

Answer: a

11.Which NERC CIP standard “ensures the identification, classification, response, and reporting of cybersecurity incidents related to critical cyber assets?”

- a.Physical security of critical cyber assets
- b.Systems security management
- c.Recovery plans for critical cyber assets
- d.Incident reporting and response planning

Answer: d

12.In NIST SP 800-53, the security controls are divided into 17 families, each with a unique, two-character identifier. The control families are themselves partitioned into three classes. Which of the three classes does the control family titled CP (contingency planning) fall under?

- a.Technical
- b.Management
- c.Operational
- d.Administrative

Answer: c

13.The NIST SP 800-53 controls are considered baseline controls, which can be tailored to more closely meet the needs of a particular organization and automation system. Which of the following is NOT one of the elements of the NIST SP 800-53 tailoring process?

- a.Selecting (or specifying) compensating security controls, if needed, to adjust the preliminary set of controls to obtain an equivalent set deemed to be more feasible to implement
- b.Applying scoping guidance to the initial baseline security controls to obtain a preliminary set of applicable controls for the tailored baseline
- c.Specifying organization-defined parameters in the security controls via explicit assignment and selection statements to complete the definition of the tailored baseline
- d.Developing custom parameters to meet the needs of the control system

Answer: d

14.The NIST SP 800-53 tailoring process refers to guidance “designed to ensure that only the controls appropriate to the particular mission and requirements of the organization are used.” This guidance is referred to as which of the following?

- a.Correlating
- b.Assessing
- c.Evaluating
- d.Scoping

Answer: d

15.NIST SP 800-53 provides for the use of security controls, which the publication defines as “a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control ... that provides an equivalent or comparable level of protection for an information system and the information processed, stored, or transmitted by that system.” This type of additional control is known as which of the following?

- a.Supporting
- b.Supplemental

- c.Compensating
- d.Custom

Answer: c

16.Recognizing some of the special requirements of industrial automation and control systems, NIST SP 800-53 defines supplements to the baseline control systems to address automation and control issues. Which one of the following is NOT one of these supplements?

- a.Risk evaluation
- b.Predictable failure prevention
- c.Emergency power
- d.Access enforcement

Answer: a

17.The Department of Homeland Security's *Catalog of Control Systems Security* is based on which of the following security controls documents?

- a.NIST SP 800-82
- b.NIST SP 800-53
- c.NIST SP 800-39
- d.The NERC CIP Cybersecurity Standards

Answer: b

18.The Advanced Metering Infrastructure (AMI) Security Requirements are characterized by letters. Which of the following is NOT one of the AMI security requirements categories?

- a.“R” are risk requirements
- b.“F” are functional requirements
- c.“S” are supporting services to functional requirements
- d.“A” are assurance requirements

Answer: a

19.The Advanced Metering Infrastructure (AMI) security requirement FIN refers to which of the following security principles?

- a.Inventory

- b.Final evaluation
- c.Integrity
- d.Internal

Answer: c

20.The recording of activity by actors/elements throughout the system and providing the means to perform a successful audit of events that occur on the system refers to which of the following Advanced Metering Infrastructure (AMI) security controls?

- a.Accounting
- b.Anomaly detection
- c.Authentication
- d.Authorization

Answer: a

21.Which of the following is NOT one of the Department of Defense Instruction 8500.2 security control subject areas?

- a.Security design and configuration
- b.Risk management
- c.Physical and environmental
- d.Continuity

Answer: b

22.Department of Defense Instruction 8500.2, control CODP, Disaster and Recovery Planning, provides which of the following information security principles?

- a.Availability
- b.Integrity
- c.Accountability
- d.Authentication

Answer: a

23.In NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, risk assessment, planning, systems and services acquisition, certification, accreditation, and security assessments fall

under what category of controls?

- a.Technical
- b.Logical
- c.Management
- d.Operational

Answer: c

24.In NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, controls such as personnel security and contingency planning fall under which of the following control categories?

- a.Management
- b.Operational
- c.Technical
- d.Physical

Answer: b

25.In NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, controls, such as identification and authentication, access control, and audit and accountability fall under which of the following control categories?

- a.Administrative
- b.Operational
- c.Management
- d.Technical

Answer: d

26.ANSI/ISA-TR99.00.01-2007, *Security Technologies for Industrial Automation and Control Systems*, defines which of the following principles as “the process of positively identifying potential network users, hosts, applications, services, and resources, using a combination of identification factors or credentials. The result of this process then becomes the basis for permitting or denying further actions”?

- a.Authentication
- b.Authorization
- c.Accountability

d.Accessibility

Answer: a

27.ANSI/ISA-TR99.00.01-2007, *Security Technologies for Industrial Automation and Control Systems*, divides authentication into which of the following two areas?

- a.User authentication and group authentication
- b.Group authentication and network service authentication
- c.User authentication and network service authentication
- d.Platform authentication and user authentication

Answer: c

28.ANSI/ISA-TR99.00.01-2007 defines which of the following as “can be used to distinguish communication by devices that are not part of the desired network. This feature is generally attractive for SCADA and other process control systems that wish to allow little or no access to the control network, but is difficult to deploy in systems requiring unrestricted Internet access”?

- a.Asymmetric key encryption
- b.Digital signature
- c.Biometrics
- d.Symmetric key encryption

Answer: d

29.ANSI/ISA-TR99.00.01-2007 states that encryption can also be employed in a virtual private network (VPN), which provides for authentication, integrity, and protection from unauthorized disclosure. Which of the following is NOT one of the most common VPN implementations?

- a.Hyper Text Transfer Protocol (HTTP)
- b.Internet Protocol Security (IPSec)
- c.Secure Shell (SSH)
- d.Secure Sockets Layer (SSL)

Answer: a

30.What standards address “the identification and protection of critical cyber assets to support reliable operation of the Bulk Electric System (BES)?”

- a.ANSI/ISA-TR99.00.01-2007
- b.NIST SP 800-53
- c.NIST SP 800-82
- d.NERC CIP Cybersecurity Standards

Answer: d

31.Which of the following is NOT one of the NERC CIP Cybersecurity Standards?

- a.Risk Management
- b.Critical Cyber Asset Identification
- c.Security Management Controls
- d.Personnel and Training

Answer: a

32.The following are characterized as what type of guidance in NIST SP 800-53: determining the primary security objectives, which system components the controls are applicable to, and what technologies are employed in the system?

- a.Custom
- b.Complementary
- c.Scoping
- d.Supplemental

Answer: c

33.In NIST SP 800-53, one of the industrial control system supplemental controls states that “it protects the information system from harm by considering mean time to failure for [*Assignment: organization-defined list of information system components*] in specific environments of operation.” This industrial control system industrial supplemental control is which of the following?

- a.Predictable Failure Prevention
- b.Fail in a Known State
- c.Access Enforcement
- d.Emergency Power

Answer: a

34.The Organizational Security controls in the Department of Homeland Security *Catalog of Control Systems Security* relate to which of the following control categories in NIST SP 800-53?

- a.Personnel Security (PS)
- b.System and Services Acquisition (SA)
- c.Access Control (AC) and Program Management (PM)
- d.Contingency Planning (CP) and Media Protection (MP)

Answer: c

35.The Monitoring and Reviewing Control System Security Policy controls in the *Catalog of Control Systems Security* relate to which of the following control categories in NIST SP 800-53?

- a.Audit and Accountability (AU)
- b.Program Management (PM)
- c.Security Assessment and Authorization (CA)
- d.System and Information Integrity (SI)

Answer: c

36.The AMI System Security Requirement that addresses “the proof of identity of an actor” is which of the following?

- a.Authentication
- b.Identification
- c.Authorization
- d.Nonrepudiation

Answer: a

37.The AMI System Security Requirement that is “based on security auditing and recognizing, recording, storing, and analyzing information related to security relevant activities” is which of the following?

- a.Authorization
- b.Authentication
- c.Accountability
- d.Integrity

Answer: c

Review Questions for Chapter 7

1.What organizations host the National SCADA Test Bed (NSTB) program?

- a.NIST and the NSA
- b.The Idaho National Laboratory and the Sandia National Laboratories
- c.ISA and SANS
- d.US-CERT and NIST

Answer: b

2.Which of the following is NOT a function of the National SCADA Test Bed (NSTB)?

- a.Assess selected control systems and control system components to identify cyber vulnerabilities
- b.Develop new standards and guidelines for governmental agencies
- c.Provide control system security training through workshops that describe common cyber vulnerabilities found in control systems
- d.Share with appropriate standards organizations information that can be used to support the development of improved industry standards applicable to control system security

Answer: b

3.What organization developed and teaches the application of 99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*?

- a.SANS
- b.NIST
- c.ISA
- d.NSA

Answer: c

4.In a training program hands-on exercise, what is the function of the Red Team?

- a.Mitigating
- b.Scanning
- c.Defending
- d.Attacking

Answer: d

5.In a training program hands-on exercise, what is the function of the Blue Team?

- a.Defending
- b.Attacking
- c.Scanning
- d.Mitigating

Answer: a

6.What is fuzzing?

- a.Modifying memory locations
- b.An attack using random or malformed bad data
- c.Scanning to determine vulnerabilities
- d.Responding to an attack by counterattacking

Answer: b

7.The National Initiative for Cybersecurity Education (NICE) is a partnership of government, industrial, educational, and professional organizations. Which of the following is NOT one of the goals of NICE?

- a.Raise awareness among the American public about the risks of online activities
- b.Broaden the pool of skilled workers capable of supporting a cyber-secure nation
- c.Develop and maintain an unrivaled, globally competitive cybersecurity workforce
- d.Develop secure digital control systems

Answer: d

8.Which of the following organizations is NOT a participant in the NICE

initiative?

- a.NIST
- b.NASA
- c.Department of Homeland Security (DHS)
- d.NSA

Answer: b

9.The NICE Cybersecurity Workforce Framework develops a vocabulary that can be used by any type of organization in categorizing cybersecurity work. Which of the following is NOT a category in this framework?

- a.Penetration testing
- b.Design
- c.Operation
- d.Maintenance

Answer: a

10.The U.S. National Centers of Academic Excellence initiative is sponsored by which of the following organizations?

- a.NIST and the Department of Energy
- b.SANS and the Department of Education
- c.NSA and the Department of Homeland Security
- d.The Department of Defense and the US-CERT

Answer: c

11.The designation of an institution as a National Center of Academic Excellence has a duration of how many years before the institution has to reapply?

- a.Two years
- b.Ten years
- c.Five years
- d.Seven years

Answer: c

12. Which of the following is NOT one of the critical steps in the life cycle of a security awareness and training program as described in NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*?

- a. Awareness and training program design
- b. Program implementation
- c. Post-implementation
- d. Pre-implementation needs review

Answer: d

13. Which of the following is NOT one of the three common models used in managing a security training function as described in NIST Special Publication 800-50?

- a. Centralized
- b. Partially Decentralized
- c. Partitioned
- d. Fully Decentralized

Answer: c

14. According to NIST SP 800-50, learning is a continuum comprising which of the following elements?

- a. Awareness, skill, knowledge
- b. Awareness, training, education
- c. Training, education, skill
- d. Education, awareness, skill

Answer: b

15. NIST SP 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model (Draft)*, defines the following as what type of training?

“Focuses on providing the knowledge, skills, and abilities specific to an individual’s roles and responsibilities relative to information systems. At this level, training recognizes the differences between beginning, intermediate, and advanced skill requirements.”

- a. Role-based training

- b.Task-oriented training
- c.Responsibility training
- d.Knowledge and skills training

Answer: a

16.Which one of the following is NOT one of the five phases of the industrial design model described in NIST SP 800-16?

- a.Analysis
- b.Training
- c.Design
- d.Evaluation

Answer: b

17.What are the two types of evaluations in the evaluation phase of the industrial design model described in NIST SP 800-16?

- a.Formative and summative
- b.Formative and intuitive
- c.Summative and descriptive
- d.Descriptive and formative

Answer: a

Review Questions for Chapter 8

1.The technology that eliminates the binding of software to specific hardware platforms is known as which of the following?

- a.Artificial intelligence
- b.Virtualization
- c.Cloud computing
- d.Software as a service

Answer: b

2.A hypervisor is which of the following?

- a.A virtual machine monitor
- b.An advanced HMI
- c.A manager
- d.An alarm mechanism

Answer: a

3.NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, defines the process for developing an ISCM strategy and implementing an ISCM program. Which one of the following best describes the ISCM strategy?

- a.Providing security mechanisms to reduce risks to automation systems
- b.Developing security policies to specify management intent for information systems and automation systems
- c.Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions
- d.Maintaining ongoing awareness of risk mitigation alternatives

Answer: c

4.Which of the following is NOT one of the ISCM program steps?

- a.Define
- b.Establish
- c.Respond
- d.Mitigate

Answer: d

5.In the ISCM process, the status of automation security in a facility can be determined by establishing appropriate metrics. Which of the following activities is NOT used to define the metrics?

- a.Evaluating applicable mitigation approaches
- b.Assessing all security controls
- c.Providing actionable communication of security status across all tiers of the organization

d. Collecting, correlating, and analyzing security-related information

Answer: a

6. NIST SP 800-137 defines the process for managing information security and information system-related risk as which of the following?

a. Risk Management Framework (RMF)

b. Risk-Impact Criteria (RIC)

c. Vulnerability Analysis (VA)

d. Risk-Vulnerability Matrix (RVM)

Answer: a

7. Security control volatility, system categorizations/impact levels, organizational risk tolerance, and security controls with identified weaknesses are associated with what characteristic discussed in NIST 800-137?

a. The necessity of adding compensating controls

b. The risk impact levels

c. The level of risk

d. The frequency of monitoring security controls for effectiveness

Answer: d

8. Appendix D of NIST SP 800-137 defines a term as “an information security area that includes a grouping of tools, technologies, and data.” What is this term?

a. Security automation domain

b. Compensating domain

c. Risk management domain

d. Risk mitigation domain

Answer: a

9. The SEI-maintained Smart Grid Maturity Model (SGMM) is described best by which of the following statements?

a. Provides a framework for understanding the current state

of Smart Grid deployment and capability within an electric utility and provides a context for establishing future strategies and work plans as they pertain to Smart Grid implementations

- b. Provides a management perspective of Smart Grid deployment and capability within an electric utility and develops guidelines for Smart Grid implementations
- c. Provides a targeted hierarchical methodology applicable to Smart Grid evaluation and maintenance within an electric utility and provides a basis for implementing effective Smart Grid controls
- d. Provides a Smart Grid assurance model and algorithms for future deployment and implementation of Smart Grid systems

Answer: a

10. Which of the following is NOT one of the eight domains of the SGMM?

- a. Strategy, Management, and Regulatory (SMR)
- b. Organization and Structure (OS)
- c. Metering and Monitoring (MAM)
- d. Work and Asset Management (WAM)

Answer: c

11. Which of the following is NOT one of the six maturity levels defined in the SGMM?

- a. Default
- b. Evaluating
- c. Initiating
- d. Integrating

Answer: b

12. The SGMM maturity rating for each domain in an organization is determined by which of the following means?

- a. The SGMM Domain survey
- b. The SGMM Risk survey

- c.The SGMM Level survey
- d.The SGMM Compass survey

Answer: d

13.NIST 7628, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cybersecurity*, is a three-volume document that provides a methodical approach to implementing customized cybersecurity and privacy protection strategies for Smart Grid implementations. Which of the following areas is NOT addressed in the volumes comprising NISTIR 7628?

- a.Risk assessment processes
- b.Privacy issues
- c.Cost evaluation matrices
- d.Research and development topics

Answer: c

14.Which of the following describes the optimizing level (Level 4) of the SGMM?

- a.Focuses on implementing features that will enable an organization to achieve and sustain grid modernization
- b.Smart Grid implementations within a given domain are being fine-tuned and used to further increase organizational performance
- c.Smart Grid deployments are being integrated across the organization
- d.Organizations are achieving new results with a given domain and advancing the state of the practice

Answer: b

15.What entity in the SGMM is defined as “the stages of an organization’s progress toward achieving its Smart Grid vision in terms of automation, efficiency, reliability, energy and cost savings, integration of alternative energy sources, improved customer interaction, and access to new business opportunities and markets?”

- a.Maturity
- b.Capability
- c.Characteristics

d.Value

Answer: a

16.In the ISCM process, the status of automation security in a facility can be determined by establishing appropriate metrics. The metrics are defined through the following activities, except one, which is not applicable. Which of the following is NOT applicable?

- a.Maintaining an understanding of threats and threat activities
- b.Conducting security awareness training
- c.Collecting, correlating, and analyzing security-related information
- d.Active management of risk by organizational officials

Answer: b

17.What technology reduces the effort required to maintain hardware and software systems by eliminating the binding of software to specific hardware platforms through the logical partitioning of physical computing resources into multiple execution environments, including servers, applications, and operating systems?

- a.Virtualization
- b.Cloud computing
- c.Distributed computing
- d.Multi-core chips

Answer: a

18.Which of the following statements is FALSE regarding penetration testing of industrial automation and control systems?

- a.If not properly conducted, penetration testing can cause damage to automation systems and disrupt operations.
- b.Penetration testing tools do not create additional traffic on automation networks and do not affect systems with limited memory capacity.
- c.If executed properly, penetration testing can provide important information regarding the security of automation systems.
- d.It is useful to use nonintrusive methods when conducting

penetration testing.

Answer: b

19. Penetration testing conducted with no prior knowledge of the automation system is known as which of the following?

- a. Black box
- b. White box
- c. Grey box
- d. Auto box

Answer: a

20. Which of the following is NOT a component of the reconnaissance phase of penetration testing?

- a. Footprinting
- b. Scanning
- c. Controlling
- d. Enumerating

Answer: c

21. Which of the following is NOT one of the maturity levels of the Automation Maturity Model?

- a. Local digital control
- b. Remote auto control
- c. Optimized operations
- d. Enabled control

Answer: d

22. What level of the Automation Maturity Model is characterized by full automation and automated closed-loop control around a set point?

- a. Local digital control
- b. Enhanced operations
- c. Remote auto control
- d. Optimized operations

Answer: c

Glossary and Acronyms

Abuse: Malicious misuse, with the objective of intentional denial, alteration, or destruction. See misuse.

Acceptance testing: A type of testing used to determine whether or not software is acceptable to the actual users.

Access: A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Access control mechanisms: Hardware or software features, operating procedures, management procedures, and various combinations thereof that are designed to detect and prevent unauthorized access and to permit authorized access in an automated system.

Access control: The process of limiting access to system or software resources only to authorized users, programs, processes, or other systems (on a network). This term is synonymous with controlled access and limited access.

Access list: A list of users, programs, and/or processes and the specifications of access categories to which each is assigned; a list denoting which users, programs, and/or processes have what access privileges to a particular resource.

Access point (AP): A wireless LAN transceiver interface between a wireless network and a wired network. Access points forward frames between wireless devices and hosts on the LAN.

Access type: The nature of an access right to a particular device, program, or file (e.g., read, write, execute, append, modify, delete, or create).

Accountability: A property that allows auditing of IT system activities to be traced to persons or processes that may then be held responsible for their actions. Accountability includes authenticity and nonrepudiation.

Accreditation: A formal declaration by the designated approving authority (DAA) that the automated information system (AIS) is approved to operate in

a particular security mode by using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Accreditation authority: Synonymous with designated approving authority.

Acquisition: The act of procurement or purchase of a product or service under license, subscription, or contract.

Advanced Encryption Standard (AES) (originally, Rijndael): A symmetric block cipher with a block size of 128 bits, in which the key can be 128, 192, or 256 bits. The Advanced Encryption Standard replaces the Data Encryption Standard (DES) and was announced on November 26, 2001 as Federal Information Processing Standard Publication 197 (FIPS PUB 197).

AIS: Automated information system.

API: Application programming interface.

Application layer: The top layer of the Open Systems Interconnection (OSI) model, which is concerned with application programs. It provides services such as file transfer and email to the network's end users.

Application process: An entity, either human or software, that uses the services offered by the application layer of the OSI reference model.

Application programming interface (API): An interface to a library of software functions. An API is designed to allow software developers to call functions from the library and to make requests of an operating system or another software component.

Application software: Software that accomplishes functions such as database access, electronic mail, and menu prompts.

Architecture: When referring to a computer system, architecture describes the type of components, interfaces, and protocols the system uses and how they fit together. It is the configuration of any equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment, and services, including support services and

related resources.

Asset: An object of value. In the context of this book, an asset could be a computer system, network, PLC, plant equipment, controllers, data acquisition systems, and so on.

Assurance: A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy; the grounds for confidence that an IT product or system meets its security objectives.

Asymmetric (public) key encryption: Cryptographic system that employs two keys, a public key and a private key. The public key is made available to anyone wishing to send an encrypted message to an individual holding the corresponding private key of the public-private key pair. Any message encrypted with one of these keys can be decrypted with the other. The private key is always kept private. It should not be possible to derive the private key from the public key.

Asynchronous transmission: The transmission of data at a variable bit rate without the use of an external clock signal and the timing required to decode the data is contained within the communication stream.

Attack: The act of trying to bypass security controls on a system. An attack can be active, resulting (or potentially resulting) in data modification, or passive, resulting (or potentially resulting) in the release of data. *Note:* The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.

Audit trail: A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to its final result.

Authenticate: (1) To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to system resources; (2) To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Authentication: The process of verifying “who” is at the other end of a transmission.

Authentication device: A device whose identity has been verified during the

lifetime of the current link based on the authentication procedure.

Authenticity: A property that allows the ability to validate the claimed identity of a system entity.

Authorization: The granting of access rights to a user, program, or process.

Automated information system (AIS): An assembly of computer hardware, software, and/or firmware that is configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Automated information system security: Measures and controls that protect an AIS against denial of service (DoS) and unauthorized (accidental or intentional) disclosure, modification, or destruction of an AIS and data. AIS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computers and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls that are needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS.

Automated security monitoring: The use of automated procedures to ensure that security controls are not circumvented.

Availability: Refers to the ability of an authorized person or process to have prompt and reliable access to computational resources, when needed.

Availability of data: The condition in which data is in the place needed by the user, at the time the user needs it, and in the form needed by the user.

Backbone network: A network that interconnects other networks.

Back door: Synonymous with trap door.

Backup plan: Synonymous with contingency plan.

Bandwidth: Specification of the amount of the frequency spectrum that is usable for data transfer. In other words, bandwidth is the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power). Also, the amount of information that may be sent

through a connection.

Bell-LaPadula model: A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined, and each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system is secure. A system state is defined to be secure only if the permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object, and a determination is made as to whether the subject is authorized for the specific access mode. Also see * property (or star property) and simple security property.

Between-the-lines entry: Unauthorized access obtained by tapping the temporarily inactive terminal of a legitimate user. See piggyback.

Binary digit: See bit.

Biometrics: Access control method in which an individual's physiological or behavioral characteristics are used to determine that individual's access to a particular resource.

BIOS: Basic input/output system. The BIOS is the first program to run when the computer is turned on. BIOS initializes and tests the computer hardware, loads and runs the operating system, and manages setup for making changes in the computer.

Bit: Short for binary digit. A single digit number in binary (0 or 1).

Bit decay: The gradual loss of information stored in bits on storage media over time.

Bit splitting: Splitting bits into groups of bits and processing the groups such that after they are recombined the correct result is obtained. A countermeasure to a differential power analysis attack that does not expose the target bits internally to the processor, so the power trace is not affected.

Black box test: A test of system security in which an ethical hacking team has no knowledge of the target network.

Black hat hacker: A hacker who conducts unethical and illegal attacks

against information systems to gain unauthorized access to sensitive information.

Block cipher: A symmetric key algorithm that operates on a fixed-length block of plaintext and transforms it into a fixed-length block of ciphertext. A block cipher is obtained by segregating plaintext into blocks of n characters or bits and applying the same encryption algorithm and key to each block.

Browsing: The act of searching through storage to locate or acquire information without necessarily knowing the existence or the format of the information being sought.

BSI ISO/IEC 17799:2000, BS 7799-I: 2000, “Information Technology—Code of Practice for Information Security Management.” British Standards Institution, London, UK: A standard intended to “provide a comprehensive set of controls comprising best practices in information security.” ISO refers to the International Organization for Standardization, and IEC is the International Electrotechnical Commission.

Buffer overflow: A condition in which more input is placed into a buffer or data holding area than the allowed or allocated capacity, overwriting other information. Such a condition is exploited by attackers to crash or gain control of a system.

Bug: An error, defect, mistake, vulnerability, failure, or fault in a computer system or in software.

Byte: A set of bits, usually eight, that represent a single character.

C&A: Certification and accreditation.

CA: Certificate authority/agent. See certificate authority.

Calls: The operations performed by an application to perform a task.

Call graph: A visual representation of a sequence of calls.

Capability: A protected identifier that identifies an object and specifies the access rights allowed to the accessor who possesses the capability. In a capability-based system, access to protected objects (such as files) is granted if the would-be accessor possesses a capability for the object.

CAPI: See cryptographic application programming interface.

Category: A restrictive label that has been applied to classified or unclassified data as a means of increasing the protection of the data and further restricting its access.

CBC: See cipher-block chaining.

CC: See Common Criteria.

CDDI: See copper data distributed interface.

Cell: See lines, units, cells.

Central processing unit (CPU): The microprocessor unit or units responsible for interpreting and executing instructions in a computer system.

Computer Emergency Response Team Coordination Center (CERT/CC): A unit of the Carnegie Mellon University Software Engineering Institute (SEI). SEI is a federally funded R&D center. CERT's mission is to alert the Internet community to vulnerabilities and attacks and to conduct research and training in the areas of computer security, including incident response.

Certification: The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Certificate authority (CA): The official responsible for performing the comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements.

Certificate revocation list (CRL): A list of certificates that have been revoked or are no longer valid and should not be relied upon.

Channel: Specific communication link established within a communication conduit. See conduit.

Cipher-block chaining (CBC): An encryption mode of the Data Encryption

Standard (DES) that operates on plaintext blocks 64 bits in length. Each block of plaintext is Exclusive ORed (XORed) with the previous ciphertext block before being encrypted. See Exclusive OR.

Cipher: A cryptographic transformation that operates on characters or bits.

Ciphertext or cryptogram: An unintelligible encrypted message.

Client: A computer that accesses a server's resources.

Client/server architecture: A network system design in which a processor or computer designated as a file server or database server provides services to other client processors or computers. Applications are distributed between a host server and a remote client.

Cluster: A group of computers linked together over a fast local area network or other means. Clustered computers work closely together such that they act and appear like a single large computer. Clusters are typically created to improve availability, performance, or redundancy beyond that provided by a single computer.

Collision: An event in which simultaneous transmissions on a communications medium interfere with one another or "collide."

Component Object Model (COM): A Microsoft technology that enables software components to communicate with each other.

Common Criteria (CC): A standard for specifying and evaluating the features of computer products and systems.

Common Object Request Broker Architecture (CORBA): A standard that uses the object request broker (ORB) to implement exchanges among objects in a heterogeneous, distributed environment.

Communications security (COMSEC): Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material and information.

Component: A constituent element of a larger system. In software, a component is a functional part of a larger program.

Compromise: A violation of a system's security policy such that unauthorized disclosure of sensitive information might have occurred.

Compromising emanations: Unintentional data-related or intelligence-bearing signals that, when intercepted and analyzed, disclose the information transmission that is received, handled, or otherwise processed by any information processing equipment. See TEMPEST.

Computer abuse: The misuse, alteration, disruption, or destruction of data-processing resources. The key is that computer abuse is intentional and improper.

Computer cryptography: The use of a crypto-algorithm in a computer, microprocessor, or microcomputer to perform encryption or decryption in order to protect information or to authenticate users, sources, or information.

Computer facility: The physical structure housing data processing operations.

Computer forensics: Collection of information from and about computer systems that is admissible in a court of law.

Computer fraud: Computer-related crimes involving deliberate misrepresentation, alteration, or disclosure of data in order to obtain something of value (usually monetary gain). A computer system must have been involved in the perpetration or cover-up of the act or series of acts. A computer system might have been involved through improper manipulation of input data, output or results, application programs, data files, computer operations, communications, computer hardware, systems software, or firmware.

Computer security (COMPUSEC): Synonymous with automated information system security.

Computing environment: The total environment in which an automated information system, network, or component operates. The environment includes physical, administrative, and personnel procedures as well as communication and networking relationships with other information systems.

COMSEC: See communications security.

Concealment: Keeping a secret attribute of a program hidden to prevent it from being discovered by an attacker.

Conduit: The means by which something is transmitted or conveyed, such as information.

Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices. The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

Configuration control: The process of controlling modifications to the system's hardware, firmware, software, and documentation in a way that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. Compare with configuration management.

Configuration management: The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the development and operational life of the system. Compare with configuration control.

Confinement: The prevention of the leaking of sensitive data from a program.

Confinement property: Synonymous with star property (* property).

Conformance testing: Planned activities to ensure that software processes and products conform to applicable requirements, standards, and procedures.

Connection-oriented service: Service that establishes a logical connection that provides flow control and error control between two stations that need to exchange data.

Connectivity: The condition of establishing and maintaining a connection between two or more points in a telecommunications system.

Containment: Preventing a successful attack on a software system from spreading to other parts of an organization's computing resources.

Contamination: The intermixing of data at different sensitivity and need-to-know levels. The lower-level data is said to be contaminated by the higher-level data, with the result that the contaminating (higher-level) data might not receive the required level of protection.

Contingency management: Establishing actions to be taken before, during,

and after a threatening incident.

Contingency plan: A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program; this plan ensures the availability of critical resources and facilitates the continuity of operations in an emergency situation. Synonymous with backup plan, disaster plan, emergency plan.

Control center: Central location used to operate a set of physical assets. *Note:* Infrastructure industries typically use one or more control centers to supervise or coordinate their operations. If there are multiple control centers (e.g., a backup center at a separate site), they are typically connected via a wide area network. The control center in such industries typically contains the SCADA host computers and associated operator display devices plus ancillary information systems such as a historian.

Control equipment: Class that includes distributed control systems, programmable logic controllers, SCADA systems, associated operator interface consoles, and field sensing and control devices used to manage and control the process. *Note:* The term also includes fieldbus networks where control logic and algorithms are executed on intelligent electronic devices that coordinate actions with each other, as well as systems used to monitor the process and the systems used to maintain the process.

Control network: Time-critical network that is typically connected to equipment that controls physical processes. *Note:* The control network can be subdivided into zones, and there can be multiple separate control networks within one company or site.

Controlled access: Synonymous with access control.

Correctness: If software performs all of its intended functions as specified, it is said to be correct, and exhibits the property of correctness.

Continuity of operations: Maintenance of essential functions and services under a broad range of circumstances.

Controlled sharing: The condition that exists when access control is applied to all users and components of a system. See access control.

Copper Data Distributed Interface (CDDI): A version of FDDI specifying the use of unshielded twisted pair wiring. See FDDI.

CORBA: See Common Object Request Broker Architecture.

Cost-risk analysis: The assessment of the cost of providing data protection for a system versus the cost of losing or compromising the data.

COTS: Commercial off-the-shelf. Refers to commercial items that are sold in substantial quantities in the commercial marketplace,

Countermeasure: Any action, device, procedure, technique, or other reactive measure that reduces the vulnerability of or threat to a system.

Covert channel: A communications channel that enables two cooperating processes to transfer information in a manner that violates the system's security policy.

Covert storage channel: A covert channel that comprises the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) shared by two subjects at different security levels.

Covert timing channel: A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.

CPU: See central processing unit.

Criteria: Standards by which something can be judged or decided. Also, see DoD Trusted Computer System Evaluation Criteria (TCSEC).

CRC: See cyclic redundancy check.

CRL: See certificate revocation list.

Cryptanalysis: The formal term for attacking cryptographic systems. In cryptanalysis, an attacker attempts to obtain the original, unencrypted message (plaintext) from the encrypted message (ciphertext).

Crypto-algorithm: A well-defined procedure, sequence of rules, or steps used to produce a keystream or ciphertext from plaintext, and vice versa. A step-by-step procedure that is used to encipher plaintext and decipher cipher-text.

Also called a cryptographic algorithm.

Cryptographic application programming interface (CAPI): An interface to a library of software functions that provide security and cryptography services. CAPI is designed for software developers to call functions from the library, which makes it easier to implement security services.

Cryptography: The principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form. The word cryptography comes from the Greek *kryptos*, meaning “hidden,” and *graphein*, “to write.”

Cryptosystem: A set of transformations from a message space to a cipher-text space. This system includes all cryptovariables (keys), plaintexts, and ciphertexts associated with the transformation algorithm (crypto-algorithm).

Cryptovariable: See key.

CSS: See DeCSS.

Cyclic redundancy check (CRC): A common error-detection process used in control systems. A mathematical operation is applied to the data when it is transmitted. The result is appended to the core packet. Upon receipt, the same mathematical operation is performed and the result is checked against the CRC. A mismatch indicates a very high probability that an error has occurred during transmission.

DAA: See designated approving authority.

Damage potential: The level of harm the attacker can cause to a system in conducting an attack.

DAC: See discretionary access control.

Data dictionary: A database that comprises tools to support the analysis, design, and development of software and to support good software engineering practices.

Data Encryption Standard (DES): A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology (NIST), is intended for public and government use.

Data flow control: See information flow control.

Data integrity: The attribute of data that is related to the preservation of its meaning and completeness, the consistency of its representation(s), and its correspondence to what it represents. Data is said to have integrity when it meets a prior expectation of quality.

Data link layer: The OSI level that performs the assembly and transmission of data packets, including error control.

Data security: The protection of data from unauthorized (whether accidental or intentional) modification, destruction, or disclosure.

Database: A persistent collection of data items that form relationships among each other.

Datagram service: A connectionless form of packet switching whereby the source does not need to establish a connection with the destination before sending data packets.

DCOM: See Distributed Component Object Model.

Decipher: To reverse the encipherment process in order to make an encrypted message human readable.

Declassification of AIS storage media: An administrative decision or procedure to remove or reduce the security classification of the subject media.

DeCSS: A program that bypasses the Content Scrambling System (CSS) software used to prevent the viewing of DVD movie disks on unlicensed platforms.

Default: A value or option that is automatically chosen when no other value or option is specified.

Degauss: To degauss a magnetic storage medium is to remove all the data stored on it by demagnetization. A degausser is a device used for this purpose.

Degausser products list (DPL): A list of commercially produced degaussers that meet National Security Agency specifications. This list is included in the NSA Information Systems Security Products and Services Catalogue and is available through the Government Printing Office.

Demilitarized zone (DMZ): A host or network segment inserted as a “neutral zone” between an organization’s private network and the Internet.

Denial of service (DoS): Any action (or series of actions) that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction or modification of data or delay of service.

Dependability: A desirable condition of software that can be attained with justifiable confidence when the software functions as intended.

DES: See data encryption standard.

Designated approving authority (DAA): The official who has the authority to decide whether to accept the security safeguards prescribed for an AIS, or the official who is responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Developer: The organization or individual that develops the information system.

DHCP: See dynamic host configuration protocol.

Dial-up: A service whereby a computer terminal can use a telephone to initiate and effect communication with a computer.

Diffusion: A method of obscuring redundancy in plaintext by dissipating the statistical structure of plaintext over the bulk of ciphertext.

Digital Millennium Copyright Act (DMCA) of 1998: Addresses copyright licensing and ownership and prohibits trading, manufacturing, or selling in any way that is intended to bypass copyright protection mechanisms.

Direct-sequence spread spectrum (DSSS): A method of spread spectrum modulation for digital signal transmission over the airwaves. The transmission is split into 14 channels, each with a frequency range, by combining a data signal with a chipping sequence. The chipping sequence or chipping code, as it is sometimes known, divides the data according to a spreading ratio. The redundant chipping code helps the signal resist interference and also enables the original data to be recovered if data bits are damaged during transmission. Data rates of 1, 2, 5.5, and 11 Mbps are obtainable.

Disaster: A sudden, unexpected, calamitous event that produces great

damage or loss; any event that creates an inability on an organization's part to provide critical business functions for some undetermined period of time.

Disaster plan: Synonymous with contingency plan.

Disaster recovery plan: Procedure for emergency response, extended backup operations, and post-disaster recovery when an organization suffers a loss of computer resources and physical facilities.

Discretionary access control (DAC): A means of restricting access to objects based on the identity and need-to-know of the user, process, and/or groups to which they belong. The controls are discretionary in the sense that a subject that has certain access permissions is capable of passing that permission (perhaps indirectly) on to any other subject. Compare with mandatory access control.

Disk image backup: The process of conducting a bit-level copy of a disk, sector by sector, which provides the capability to examine slack space, undeleted clusters, and (possibly) deleted files.

Distributed control system: A type of control system in which the system elements are dispersed but are operated in a coupled manner. *Note:* Distributed control systems may have shorter coupling time constants than those typically found in SCADA systems. *Note:* Distributed control systems are commonly associated with continuous processes such as electric power generation, oil and gas refining, chemical, and paper manufacturing as well as discrete processes such as automobile and other goods manufacturing, packaging, and warehousing.

Distributed Component Object Model (DCOM): A distributed object model that is similar to the Common Object Request Broker Architecture (CORBA). DCOM is the distributed version of COM that supports remote objects as if the objects reside in the client's address space. A COM client can access a COM object through the use of a pointer to one of the object's interfaces and then invoke methods through that pointer.

DITSCAP: See DoD Information Technology Security Certification and Accreditation Process.

DMCA: See Digital Millennium Copyright Act of 1998.

DNS enumeration: Gathering information on domain name service (DNS) servers.

DoD: U.S. Department of Defense.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP): Establishes for the defense entities a standard process, set of activities, general task descriptions, and management structure to certify and accredit IT systems that will maintain the required security posture.

DoD Trusted Computer System Evaluation Criteria (TCSEC): A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that process and/or store sensitive or classified data. This document is Government Standard DoD 5200.28-STD and is frequently referred to as “the Criteria” (see criteria) or “the Orange Book.”

Domain: The unique context (e.g., access control parameters) in which a program is operating; in effect, the set of objects that a subject has the ability to access. See process and subject.

DoS: See denial of service.

DoS attack: Denial-of-service attack.

DPL: See degausser products list.

DSSS: See direct-sequence spread spectrum.

Due care: The care which an ordinary prudent person would have exercised under the same or similar circumstances. The terms due care and reasonable care are used interchangeably.

Dynamic host configuration protocol (DHCP): A protocol that issues Internet Protocol (IP) addresses automatically within a specified range to devices such as PCs when they are first powered on. The device retains the use of the IP address for a specific license period that the system administrator can define.

EAL: See evaluation assurance level.

Electronics Industry Association (EIA): A U.S. standards organization that represents a large number of electronics firms.

Emanations: See compromising emanations.

Embedded software: Software that is an element of a larger system and performs some of the requirements of that system, such as controlling, measuring, or monitoring the actions of the system's physical components.

Embedded system: A system that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem.

Emergency plan: Synonymous with contingency plan.

Emission(s) security (EMSEC): The protection resulting from all measures taken to deny unauthorized persons information of value derived from the intercept and analysis of compromising emanations from crypto-equipment or an IT system.

Encipher: To make a message unintelligible to all but the intended recipients.

End-to-end encryption: Encrypted information sent from the point of origin to the final destination. In symmetric key encryption, this process requires the sender and the receiver to have identical keys for the session.

Enumeration: Gathering detailed information about a target information system.

Environment: The aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system.

Equipment under control: Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

Erasure: A process by which a signal recorded on magnetic media is removed. Erasure is accomplished in two ways: (1) by alternating current erasure, by which the information is destroyed when an alternating high and low magnetic field is applied to the media; (2) by direct current erasure, in which the media is saturated by applying a unidirectional magnetic field. See degauss.

Error: An error occurs (1) if an individual interacts with a software system and creates an error, for example, a coding error or an operational failure; (2) when the value actually produced by the software is different than the correct value; (3) when one of the software's states changes from correct to incorrect.

Ethernet switch: Ethernet switches establish a data link in which a circuit or a channel is connected to an Ethernet network. Switches are used to interconnect different LANs. A switch operates in the data link layer of the ISO/OSI Reference model.

Ethical hacker: Trusted individual who performs penetration tests without malicious intent.

Evaluation: Assessment of an IT or IACS against defined security functional and assurance criteria, performed by a combination of testing and analytic techniques.

Event: Something that occurs, such as a specific situation or an activity. Within a software system, an event handler is a subroutine that handles input received from the software.

Execution environment: The entities in software's operational environment such as servers, middleware, and network devices that support, affect or influence its execution.

Exploit: To exploit means to take advantage of a security weakness in software in order to compromise the software to, for example, gain control of a system. An exploit also refers to the portion of code, data, or sequence of commands used to conduct an attack.

Evaluation assurance level (EAL): In the Common Criteria, the degree of examination of the product to be tested. EALs range from EA1 (functional testing) to EA7 (detailed testing and formal design verification). Each numbered package represents a point on the CC's predefined assurance scale. An EAL can be considered a level of confidence in the security functions of an IT product or system.

Exclusive OR: A Boolean function where the output is a logical 0 when two input bits are identical (both 1's or both 0's) and the output is a logical 1 when the two input bits are not identical (one input is a 0 and the other input is a 1).

Executive state: One of several states in which a system can operate and the only one in which certain privileged instructions can be executed. Such instructions cannot be executed when the system is operating in other (e.g., user) states. Synonymous with supervisor state.

Exploitable channel: Any information channel that is usable or detectable by subjects that are external to the trusted computing base, whose purpose is to

violate the security policy of the system. See covert channel.

Exposure: An instance of being exposed to losses from a threat.

External dependencies: The network and architectural components that a network interacts with but does not control.

Fail-over: A condition in which operations automatically switch over to a backup system when one system/application fails.

Fail safe: If a failure occurs, the system should fail in a secure manner, i.e., security controls and settings remain in effect and are enforced. It is usually better to lose functionality rather than security.

Fail secure: A system design principle that preserves a secure state during and after the occurrence of failures.

Failure: A condition that occurs when software or hardware are unable to perform their intended functions within the operational parameters specified for those functions.

False negative: A condition that happens when a security tool does not report a weakness where one is present.

False positive: A condition that happens when a security tool reports a weakness where no weakness is present.

False positive rate: The number of false positives divided by the sum of the number of false positives and the number of true positives.

Fault: A condition that causes a device or system component to fail to perform in the required manner.

FCC: Federal Communications Commission.

FDMA: Frequency division multiple access. A spectrum-sharing technique whereby the available spectrum is divided into a number of individual radio channels.

FDX: See full-duplex.

Federal Intelligence Surveillance Act (FISA) of 1978: An act that limited wiretapping for national security purposes as a result of the Nixon administration's history of using illegal wiretaps.

Fetch protection: A system-provided restriction to prevent a program from accessing data in another user's segment of storage.

Fiber-Distributed Data Interface (FDDI): A set of ANSI and ISO standards for data transmission on fiber optic lines in a local area network (LAN) that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users. FDDI is frequently used on the backbone for a wide area network (WAN).

Fiestel cipher: An iterated block cipher that encrypts by breaking a plaintext block into two halves and, with a subkey, applying a "round" transformation to one of the halves. The output of this transformation is then XORed with the remaining half. The round is completed by swapping the two halves.

FIFO: See first in, first out.

File server: A computer that provides network stations with controlled access to sharable resources. The network operating system (NOS) is loaded on the file server, and most sharable devices, including disk subsystems and printers, are attached to it.

File protection: The aggregate of all processes and procedures in a system designed to inhibit unauthorized access, contamination, or elimination of a file.

File security: The means by which access to computer files is limited to authorized users only.

File Transfer Protocol (FTP): A TCP/IP protocol for file transfer.

FIPS: Federal Information Processing Standards. A set of standards that describe document processing, encryption algorithms and other information technology standards for use within nonmilitary government agencies and by government contractors and vendors who work with the agencies.

Firewall: A network device that shields a trusted network from unauthorized users in an untrusted network by blocking specific types of traffic. Many types of firewalls exist, including packet filtering and stateful inspection.

Firmware: Executable programs stored in nonvolatile memory.

First in, first out (FIFO): In computing, a method of processing elements in a queue on a first-come, first-served basis.

Flaw: A shortcoming in software's requirements, architecture, or design specification that results in a weak design or errors in the implementation. A flaw may or may not be a vulnerability.

Flow-sensitive analysis: Analysis of a computer program that takes into account the flow of control.

Flow control: See information flow control.

Footprinting: Gathering information in both active and passive modes.

Formal method: A technique used to verify, through the use of mathematical proofs, that software is consistent with its specified requirements, architecture, design, or security policy.

Formal proof: A complete and convincing mathematical argument presenting the full logical justification for each proof step for the truth of a theorem or set of theorems.

Formal security policy model: A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a secure state of the system. To be acceptable as a basis for a TCB (see TCB), the model must be supported by a formal proof that if the initial state of the system satisfies the definition of a secure state and if all assumptions required by the model hold, then all future states of the system will be secure. Some formal modeling techniques include state transition models, denotational semantics models, and algebraic specification models. See Bell-LaPadula model.

Formal verification: The process of using formal proofs to demonstrate the consistency between a formal specification of a system and a formal security policy model (design verification) or between the formal specification and its high-level program implementation (implementation verification).

Frequency division multiple access: See FDMA.

FTP: See File Transfer Protocol.

Full-duplex (FDX): Communications method where information can be transmitted in both directions simultaneously.

Functional testing: The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation.

Gateway: A network component that provides interconnectivity at higher network layers.

Gigabyte (GB, Gbyte): A unit of measure for memory or disk storage capacity; usually 1,073,741,824 bytes.

Gigahertz (GHz): A measure of frequency; one billion hertz.

GOTS: Government off-the-shelf software.

Gramm-Leach-Bliley (GLB) Act of November 1999: An act that removed Depression-era restrictions on banks that limited certain business activities, mergers, and affiliations. It repealed the restrictions on banks affiliating with securities firms contained in sections 20 and 32 of the Glass-Steagall Act. GLB became effective on November 13, 2001. GLB also requires health plans and insurers to protect member and subscriber data in electronic and other formats. These health plans and insurers will fall under new state laws and regulations that are being passed to implement GLB because GLB explicitly assigns enforcement of the health plan and insurer regulations to state insurance authorities (15 U.S.C. §6805). Some of the privacy and security requirements of Gramm-Leach-Bliley are similar to those of HIPAA (Health Insurance Portability and Accountability Act).

Granularity: An expression of the relative size of a data object; for example, protection at the file level is considered coarse granularity, whereas protection at the field level is considered to be of a finer granularity.

Gray box test: A test in which the ethical hacking team has partial knowledge of the target information system.

Gray hat hacker: A hacker who normally performs ethical hacking but sometimes reverts to malicious, black hat hacking.

Guard: A processor that provides a filter between two disparate systems operating at different security levels or between a user terminal and a database in order to filter out data that the user is not authorized to access.

Hamming weight: The Hamming weight of a string is the number of symbols that are different from the zero-symbol of the alphabet used.

Handshaking procedure: A dialogue between two entities (e.g., a user and a computer, a computer and another computer, or a program and another program) for the purpose of identifying and authenticating the entities to one another.

Hertz (Hz): A unit of frequency measurement; one cycle of a periodic event per second. Used to measure frequency.

HIPAA (Health Insurance Portability and Accountability Act): See Kennedy-Kassebaum Act of 1996.

Host: A time-sharing computer accessed via terminals or terminal emulation; a computer to which an expansion device attaches.

HTTP: Hypertext Transfer Protocol. An application layer protocol designed within the framework of the Internet Protocol suite that is the fundamental protocol of the World Wide Web.

Hypertext markup language (HTML): A standard used on the Internet for defining hypertext links between documents.

I&A: Identification and authentication. Identification is the process of presenting the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. Authentication is verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

IA: Information assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IAC: Inquiry access code; used in inquiry procedures. The IAC can be one of two types: a dedicated IAC for specific devices or a generic IAC for all devices.

ICV: Integrity check value. In Wired Equivalent Privacy (WEP) encryption, the frame is run through an integrity algorithm, and the generated ICV is placed at the end of the encrypted data in the frame. Then the receiving station runs the data through its integrity algorithm and compares it to the

ICV received in the frame. If it matches, the unencrypted frame is passed to the higher layers. If it does not match, the frame is discarded.

ID: Common abbreviation for “identifier” or “identity.”

Identification: The process that enables a system to recognize an entity, generally by the use of unique machine-readable user names.

Identity: The label applied to the type of service provided by a software component, for example, NETWORK_SERVICE.

IDS: Intrusion detection system. Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations).

IEEE: See Institute of Electrical and Electronic Engineers.

IETF: Internet Engineering Task Force. The Internet Engineering Task Force is a volunteer body that develops and promotes Internet standards. The mission of the IETF is to improve the Internet by producing high-quality, relevant technical documents that influence the way the Internet is designed, used, and managed.

IKE: Internet key exchange. The protocol used to set up a security association (SA) in the IPsec protocol suite in order to establish secure communications.

Impersonating: Synonymous with spoofing.

Implementation: The phase in the software life cycle when the software is coded from specifications and/or integrated from components.

Incomplete parameter checking: A method used to detect system design flaws that result when all parameters have not been fully examined for accuracy and consistency, thus making the system vulnerable to penetration.

Individual accountability: The ability to identify an individual and to hold that individual responsible for his or her actions.

Industrial automation and control system: Collection of personnel, hardware, and software that can affect or influence the safe, secure, and

reliable operation of an industrial process. *Note:* These systems include, but are not limited to:

- a.industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety instrumented system [SIS] functions, whether they are physically separate or integrated.)
- b.associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems.
- c.associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Industrial, scientific, and medicine (ISM) bands: Radio frequency bands authorized by the Federal Communications Commission (FCC) for wireless LANs used for industrial, scientific, and medicine-related purposes. The ISM bands are located at 902 MHz, 2.400 GHz, and 5.7 GHz. The transmitted power is commonly less than 600mW, and no FCC license is required.

Information flow control: A procedure undertaken to ensure that information transfers within a system are not made from a higher security level object to a lower security level object. See covert channel, simple security property, and star property (* property). Synonymous with data flow control and flow control.

Information security policy: The aggregate of public law, directives, regulations, and rules that regulate how an organization manages, protects, and distributes information. For example, the information security policy for financial data processed on DoD systems may be in U.S. Code (USC), Executive Order (EO), and DoD directives and in local regulations. The information security policy lists all the security requirements applicable to specific information.

Information system (IS): Any telecommunications or computer-related equipment or interconnected systems or subsystems of equipment used in the

acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data; includes software, firmware, and hardware.

Information system security engineering/engineer (ISSE): Process of capturing and refining information protection requirements to ensure their integration into information systems acquisition and information systems development through purposeful security design or configuration. Individual assigned responsibility for conducting information system security engineering activities.

Information system security officer (ISSO): (1) The person who is responsible to the designated approving authority (DAA) for ensuring that security is provided for and implemented throughout the life cycle of an AIS, from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal; (2) In certification and accreditation (C&A), the person responsible to the DAA for ensuring that the security of an IT system is approved, operated, and maintained throughout its life cycle in accordance with the SSAA.

Information technology (IT): The hardware, firmware, and software used as part of the information system to perform information-related functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control information.

Information technology security (ITSEC): (1) Protection of information technology against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats; (2) Protection and maintenance of confidentiality, integrity, availability, and accountability.

Infrared (IR) light: Light waves that range in length from about 0.75 to 1,000 microns; IR light operates at a lower frequency than the spectral colors but at a higher frequency than radio waves.

Inheritance (in object-oriented programming): When all the methods of one class, called a superclass, are inherited by a subclass. Thus, all messages understood by the superclass are understood by the subclass.

Input validation: Checking the data that is input to a software application for acceptable parameters such as data type, length, and range.

Inquiry access code: See IAC.

Institute of Electrical and Electronic Engineers (IEEE): A U.S.-based standards organization participating in the development of standards for data transmission systems. The IEEE has made significant progress in the establishment of standards for LANs, namely the IEEE 802 series.

Integration testing: A testing process used to verify the interface among components such as hardware or software modules as the components are installed. The testing personnel should integrate components into the network one by one and perform integration testing when necessary to ensure proper gradual integration of components.

Integrator: An organization or individual that unites, combines, or otherwise incorporates information system components with another system(s).

Integrity: (1) The quality of being in sound, unimpaired, or perfect condition; (2) A quality of an IT system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. It is composed of data integrity and system integrity; (3) Integrity is concerned with unauthorized modification of data, whether by an authorized or an unauthorized individual or process. If a message is intercepted, its contents are changed, and it is then forwarded to a receiver, integrity has been violated.

Integrity check value: See ICV.

Interdiction: See denial of service.

Inter-file analysis: Analysis of code resulting in different files that have procedural, data, or other interdependencies.

Internal security controls: Hardware, firmware, and software features within a system that restrict access to resources (hardware, software, and data) to authorized subjects only (persons, programs, or devices).

International Standards Organization (ISO): A nontreaty standards organization active in the development of international standards, such as the Open System Interconnection (OSI) network architecture.

International Telecommunications Union (ITU): An intergovernmental agency of the United States, responsible for making recommendations and

developing standards regarding telephone and data communications systems for public and private telecommunication organizations and for providing coordination for the development of international standards.

Internet: The largest network in the world. The successor to the Advanced Research Projects Agency Network (ARPANET), the Internet includes other large subnetworks. The Internet uses the TCP/IP protocol suite and connects universities, government agencies, business, industry, and individuals around the world.

Internet Protocol (IP): The Internet standard protocol that defines the Internet datagram as the information unit passed across the Internet. IP provides the basis of a best-effort packet delivery service. The Internet Protocol suite is often referred to as TCP/IP because IP is one of the two fundamental protocols, the other being the Transfer Control Protocol.

Internetwork packet exchange (IPX): Novell NetWare operating system protocol for the exchange of message packets on an internetwork. IPX passes application requests for network services to the network drives and then to other workstations, servers, or devices on the internetwork.

Intrusion detection system: See IDS.

Ionization: The act of converting an atom or molecule into an ion by adding or removing charged particles such as electrons or other ions.

Ionize: To convert an atom or molecule into an ion by adding or removing charged particles such as electrons or other ions.

IP: See Internet Protocol.

IPX: See internetwork packet exchange.

IS: See information system.

ISM bands: See industrial, scientific, and medicine bands.

Isolation: The containment of subjects and objects in a system in such a way that they are separated from one another as well as from the protection controls of the operating system.

IS: See information system.

ISO: See International Standards Organization.

ISP: Internet service provider. A commercial organization that provides user connections to the Internet for a fee.

ISSE: See information system security engineering/engineer.

ISSO: See information system security officer.

IT: See information technology.

ITSEC: See information technology security.

ITU: See International Telecommunications Union.

IV: An initialization vector (IV) is a random or pseudorandom character sequence that is used with a secret key for data encryption. The use of an IV makes it more difficult for an attacker to decipher the encrypted message.

Justifiable confidence: A high level of certainty, achieved with actions, arguments, and evidence.

Kennedy-Kassebaum Health Insurance Portability and Accountability Act (HIPAA) of 1996: A set of regulations that mandates the use of standards in health care record keeping and electronic transactions. The act requires that health care plans, providers, insurers, and clearinghouses do the following:

- Provide for restricted access by the patient to personal health care information
- Implement administrative simplification standards
- Enable the portability of health insurance
- Establish strong penalties for health care fraud

Key: Information or sequence that controls the enciphering and deciphering of messages. Also known as a cryptovvariable. Used with a particular algorithm to encipher the plaintext message or decipher the encrypted message.

Keystream: A sequence of random or pseudorandom characters that are combined with a plaintext message to produce an encrypted message (the

ciphertext).

Kilobyte (KB, Kbyte): A unit of measurement of memory or disk storage capacity; a data unit of 210 (1,024) bytes.

Kilohertz (kHz): A unit of frequency measurement; equivalent to 1,000 Hz.

Knowledge base: The rules and facts of the particular problem domain in an expert system. An expert system is a type of artificial intelligence element that makes decisions based on a knowledge base and rules derived from interviews with domain experts.

LAN: See local area network.

Least privilege: In the principle of least privilege, a user or process is given the minimum amount of privileges, authorization, and so on for the least amount of time that will permit him or her to accomplish assigned tasks and complete a mission. Least privilege reduces the prospect of an individual or process having unauthorized access to sensitive information.

Light-emitting diode (LED): Used in conjunction with optical fiber, an LED emits light when current is passed through it. Its advantages include low cost and long life, and it is capable of transmitting data in the million bits per second (Mbps) range.

Limited access: Synonymous with access control.

Lines, units, cells: Lower-level control system elements (entities) that perform manufacturing, field device control, or vehicle functions. *Note:* Entities at this level may be connected together by an area control network and may contain information systems related to the operations performed in that entity.

Local area network (LAN): A network that interconnects devices in the same office, floor, or building, or in adjacent or nearby buildings.

MAC: See mandatory access control if used in the context of a type of access control. MAC also refers to the media access control address assigned to a network interface card on an Ethernet network.

Magnetic remanence: A measure of the magnetic flux density that remains after removal of an applied magnetic force. Refers to any data remaining on magnetic storage media after removal of the power.

Mail gateway: A type of gateway that interconnects dissimilar email systems.

Maintainer: The organization or individual that maintains the information system.

Maintenance organization: The organization that keeps an IT or industrial automation and control system operating in accordance with prescribed requirements, laws, policies, procedures, and regulations.

Malicious code: Software or firmware that is intentionally included in a system for an unauthorized purpose (e.g., a Trojan horse).

Malicious logic: Synonymous with malicious code.

Malware: A merging of the words malicious and software. Malware is inserted into a system, usually covertly, with the intention of compromising the confidentiality, availability, or integrity of the system's data, applications, and operating system. It may come to the attention of a user by inhibiting the operational abilities of the system. Often referred to as malicious code.

Mandatory access control (MAC): A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (in other words, clearance) of subjects to access information of such sensitivity. Compare with discretionary access control.

Manufacturing operations: Collection of production, maintenance, and quality assurance operations and their relationship to other activities of a production facility. Manufacturing operations include:

- a.manufacturing or processing facility activities that coordinate the personnel, equipment, and material involved in the conversion of raw materials or parts into products
- b.functions that may be performed by physical equipment, human effort, and information systems
- c.managing information about the schedules, use, capability, definition, history, and status of all resources (personnel, equipment, and material) within the manufacturing facility

Masquerading: Synonymous with spoofing.

Media access control (MAC): An IEEE 802 standards sublayer used to control access to a network medium, such as a wireless LAN. Also deals with collision detection. Each computer has its own unique MAC address.

Megabits per second (Mbps): One million bits per second, typically referring to a data transmission rate.

Megabyte (MB, Mbyte): A unit of measurement for memory or disk storage capacity, usually 1,048,576 bytes.

Megahertz (MHz): A measure of frequency equivalent to one million cycles per second.

Middleware: An intermediate software component located on a wired network between a wireless appliance and the application or data residing on the wired network. Middleware provides appropriate interfaces between the appliance and the host application or server database.

Mimicking: Synonymous with spoofing.

Mission: The assigned duties to be performed by a resource.

Misuse: Use of software that deviates from what is expected based on the software's specifications. If the misuse is malicious in nature, it is typically referred to as abuse.

Mobile code: Software obtained from remote computer systems across a network, and downloaded and executed on a local computer system without explicit installation or execution by the recipient. Examples include JavaScript, Java applets, ActiveX controls, and Flash animations. Mobile code can be used for valid applications or can contain a virus that could do harm to a computer system.

Modes of operation: A description of the conditions under which an AIS functions, based on the sensitivity of the data processed and the clearance levels and authorizations of the users. Four modes of operation are authorized:

1. **Dedicated mode:** An AIS is operating in the dedicated mode when each user who has direct or indirect individual access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

- a. A valid personnel clearance for all information on the

system

b. Formal access approval; furthermore, the user has signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs)

c. A valid need-to-know for all information contained within the system

2. System-high mode: An AIS is operating in the system-high mode when each user who has direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

a. A valid personnel clearance for all information on the AIS

b. Formal access approval, and signed nondisclosure agreements, for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs)

c. A valid need-to-know for some of the information contained within the AIS

3. Compartmented mode: An AIS is operating in the compartmented mode when each user who has direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

a. A valid personnel clearance for the most restricted information processed in the AIS

b. Formal access approval, and signed nondisclosure agreements, for that information which he or she will be able to access

c. A valid need-to-know for that information which he or she will be able to access

4. Multilevel mode: An AIS is operating in the multilevel mode when all of the following statements are satisfied concerning the users who have direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts:

a. Some do not have a valid personnel clearance for all the information processed in the AIS.

b. All have the proper clearance and the appropriate formal access approval for that information to which they are to have access.

c. All have a valid need-to-know for that information to which they are to have access.

Multilevel device: A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (e.g., machine-readable or human-readable) as the data being processed.

Multilevel secure: A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know but that prevents users from obtaining access to information for which they lack authorization.

Multilevel security mode: See modes of operation.

Multiple inheritance: In object-oriented programming, a situation where a subclass inherits the behavior of multiple superclasses.

Multiuser mode of operation: A mode of operation designed for systems that process sensitive, unclassified information in which users might not have a need-to-know for all information processed in the system. This mode is also used for microcomputers processing sensitive unclassified information that cannot meet the requirements of the stand-alone mode of operation.

Mutually suspicious: A state that exists between interacting processes (subsystems or programs) in which neither process can expect the other process to function securely with respect to some property.

National Computer Security Center (NCSC): Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the widespread availability of trusted computer systems throughout the federal government. It is a branch of the National Security Agency (NSA) that also initiates research and develops and publishes standards and criteria for trusted information systems.

National Information Assurance Certification and Accreditation Process (NIACAP): Provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the information assurance and security posture of a system or site. The NIACAP is designed to certify that the information system meets documented accreditation requirements and continues to maintain the accredited security posture throughout the system life cycle. This document is issued and maintained by the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

National Institute of Standards and Technology (NIST): NIST is a nonregulatory federal agency within the U.S. Department of Commerce.

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

National Security Agency (NSA): The National Security Agency (NSA) is a cryptologic intelligence agency of the United States Department of Defense responsible for the collection and analysis of foreign communications and foreign signals intelligence, as well as protecting U.S. government communications and information systems.

NCSC: See National Computer Security Center.

Need-to-know: The necessity for access to, knowledge of, or possession of specific information that is required to carry out assigned duties in industrial automation and control systems and systems critical to national security.

Network basic input/output system (NetBIOS): A standard interface between networks and PCs that enables applications on different computers to communicate within a LAN. NetBIOS was created by IBM for its early PC network, was adopted by Microsoft, and has since become a de facto industry standard. It is not routable across a wide area network (WAN).

Network interface card (NIC): A network adapter inserted into a computer that enables the computer to be connected to a network.

Network monitoring: A form of operational support enabling network management to view the network's inner workings. Most network-monitoring equipment is nonobtrusive and can be used to determine the network's utilization and to locate faults.

NIACAP: See National Information Assurance Certification and Accreditation Process.

NIAP: See National Information Assurance Partnership.

NIST: See National Institute of Standards and Technology.

Node: Any network-addressable device on a network, such as a router or network interface card. Any network station.

Nonrepudiation: Nonrepudiation in digital systems refers to ensuring that the sender of a message or contract cannot later deny sending the message or contract and that, conversely, a receiver to whom the message was sent

cannot deny receiving the message. Digital signatures are used to implement nonrepudiation.

NSA: See National Security Agency.

Object: A passive entity that contains or receives information. Access to an object implies access to the information that it contains. Examples of objects include records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

Object request broker (ORB): The fundamental building block of the object request architecture (ORA), which manages the communications among the ORA entities. The purpose of the ORB is to support the interaction of objects in heterogeneous, distributed environments. The objects may be on different types of computing platforms.

Object reuse: The reassignment and reuse of a storage medium (e.g., page frame, disk sector, and magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (data remanence) from the object(s) that were previously contained in the media.

Object services: Services that support the ORB in creating and tracking objects as well as performing access control functions.

OMB: Office of Management and Budget. As part of the executive branch of the U.S. government, the OMB serves the president of the United States in implementing his vision across the executive branch. OMB is the largest component of the executive office of the president. It reports directly to the President and helps a wide range of executive departments and agencies across the federal government to implement the commitments and priorities of the president.

OPC: A set of specifications for the exchange of information in a process control environment. *Note:* The abbreviation “OPC” originally came from “OLE for process control,” where “OLE” was short for “object linking and embedding.”

Open security environment: An environment that includes those systems in which at least one of the following conditions holds true: (1) application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic, and (2) configuration control does not provide sufficient assurance that applications are protected against the introduction of

malicious logic prior to and during the operation of system applications.

Open source software (OSS): Software that is publicly available and is provided under a license that is less restrictive than a typical commercial license. A typical license may permit users to change the software and redistribute the software in modified or unmodified form.

Open System Interconnection (OSI): An ISO standard specifying an open system capable of enabling communications between diverse systems. OSI has the following seven layers of distinction: physical, data link, network, transport, session, presentation, and application. These layers provide the functions that enable standardized communications between two application processes.

Operating system (OS): The collection of software that directs a computer's operations, controlling and scheduling the execution of other programs, and managing storage, input/output, and communication resources.

Operations security: Controls over hardware, media, and operators who have access to computer systems. Operations security and controls safeguard information assets while the data is resident in the computer or otherwise directly associated with the computing environment. The controls address both software and hardware as well as such processes as change control and problem management.

Operator: An individual who supports system operations from the operator's console, monitors execution of the system, and controls the flow of jobs.

Orange Book: Alternate name for the DoD Trusted Computer System Evaluation Criteria.

Original equipment manufacturer (OEM): A manufacturer of products for integration into other products or systems.

ORA: Refer to the definition for object request broker.

ORB: See object request broker.

OS: Commonly used abbreviation for operating system.

OSI: See open system interconnection.

OSS: See open source software.

Overt channel: A path within a computer system or network that is designed for the authorized transfer of data. Compare with covert channel.

Overwrite procedure: A software process that replaces data previously stored on storage media with a predetermined set of meaningless data or random patterns. See magnetic remanence.

Packet: A basic message unit for communication across a network. A packet usually includes routing information, data, and (sometimes) error-detection information.

Packet-switched: (1) A type of network that routes data packets based on an address contained in the data packet. Multiple data packets can share the same network resources. (2) A type of communications network that uses shared facilities to route data packets from and to different users. Unlike a circuit-switched network, a packet-switched network does not set up dedicated circuits for each session.

Passivation layer: A protective layer that covers an integrated circuit.

Password: A protected/private character string that is used to authenticate an identity.

Penetration: The act of successfully bypassing a system's security mechanisms.

Penetration testing: The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators might be assumed to use all system design and implementation documentation, which can include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints that are applied to ordinary users.

Performance modeling: The use of simulation software to predict network behavior, allowing developers to perform capacity planning. Simulation makes it possible to model the network and impose varying levels of utilization to observe the effects.

Permissions: A description of the type of authorized interactions that a subject can have with an object. Examples of permission types include read, write, execute, add, modify, and delete.

Personnel security: (1) Procedures established to ensure that all personnel who have access to sensitive information possess the required authority as well as appropriate clearances; (2) Procedures established to evaluate a person's background; provides assurance of necessary trustworthiness.

PHI: See protected health information.

Physical security: The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

Piggyback: Gaining unauthorized access to a system via another user's legitimate connection. See between-the-lines entry.

PKI: See public key infrastructure.

Plaintext: Message text in clear, human-readable form.

Platform for Privacy Preferences (P3P): Proposed standards developed by the World Wide Web Consortium (W3C) to implement privacy practices on Web sites.

Portability: Defines network connectivity that can be easily established, used, and then dismantled.

Port scanning: Connecting to Transmission Control Protocol (TCP) and User Datagram Protocol (TCP and UDP) ports in order to determine the services and applications running on the target host.

Presentation layer: The layer of the OSI model that negotiates data transfer syntax for the application layer and performs translations between different data types, if necessary.

Private key encryption: See symmetric (private) key encryption.

Privileged instructions: A set of instructions (e.g., interrupt handling or special computer instructions) used to control features such as storage protection features that are generally executable only when the automated system is operating in the executive state.

PRNG: Pseudorandom number generator. An algorithm that produces a sequence of bits that are uniquely determined from an initial value called a

seed. The output of the PRNG “appears” to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known.

Procedural language: Comprises sequential execution of instructions based on the von Neumann architecture of a CPU, memory, and an input/output device. Variables are part of the sets of instructions used to solve a particular problem, and therefore the data is not separate from the instruction statements.

Process: (1) A program in execution. See domain and subject. (2) A series of operations performed in the making, treatment or transportation of a product or material.

Program: A plan of action aimed at accomplishing a clear technical, production, or business objective, with details on what work is to be done, by whom, when, and what means or resources will be used. In computing, a set of coded instructions that a computer executes to solve a problem or produce a desired result.

Program manager: The person ultimately responsible for the overall procurement, development, integration, modification, operation, and maintenance of an IT system.

Protected health information (PHI): Individually identifiable health information that is:

- Transmitted by electronic media
- Maintained in any medium described in the definition of electronic media (under HIPAA)
- Transmitted or maintained in any other form or medium

Protection profile (PP): In the Common Criteria, an implementation-independent specification of the security requirements and protections of a product that could be built.

Protection-critical portions of the TCB: Those portions of the TCB whose normal function is to deal with access control between subjects and objects. Their correct operation is essential to the protection of the data on the system.

Protocols: A set of rules and formats used to specify interactions between communicating entities.

Prototyping: A method of determining or verifying requirements and design specifications. The prototype normally consists of network hardware and software that support a proposed solution. The approach to prototyping is typically a trial-and-error experimental process.

Public key cryptography: See asymmetric key encryption.

Public key infrastructure (PKI): A PKI binds public keys to entities, enables other entities to verify public key bindings, and provides the services needed for ongoing management of keys in a distributed system. The goal of the PKI security architecture is to protect and distribute information that is needed in a widely distributed environment, where the users, resources, and stakeholders are in different places at different times. A PKI allows business to be conducted with the justifiable confidence that:

- The person or process sending the transaction is the actual originator.
- The person or process receiving the transaction is the intended recipient.
- Data integrity has not been compromised.

Purge: The removal of sensitive data from an automation and control system, IT system, storage device, or peripheral device with storage capacity at the end of a processing period. This action is performed in such a way that there is assurance proportional to the sensitivity of the data that the data cannot be reconstructed.

Quality: The degree to which software or hardware meets its specifications and satisfies its intended purpose.

RADIUS: See remote authentication dial-in user service.

RC4: Rivest, Shamir and Adleman (RSA) cipher algorithm 4.

Read: A fundamental operation that results only in the flow of information from an object to a subject.

Read access: Permission to read information.

Read-only memory (ROM): Computer memory on which data has been written and stored. Once data has been written onto a ROM chip, it cannot be removed and can only be read.

Recovery planning: The advance planning and preparations that are necessary to minimize loss and to ensure the availability of the critical information systems of an organization in the event of a system failure or outage/disruption.

Recovery procedures: The actions that are necessary to restore a system's computational capability and data files after a system failure or outage/disruption.

Reference-monitor concept: An access-control concept that refers to the use of an abstract machine (mechanism) that mediates all access to objects by subjects.

Reference-validation mechanism: An implementation of the reference monitor concept. A security kernel is a type of reference-validation mechanism.

Regression testing: Testing process used to ensure that existing software functions of the product have not been accidentally damaged as an unintended by-product of adding additional software features.

Relevancies: Attributes of a software component that are applicable to its attack surface. A system's attack surface is the set of ways in which an adversary can enter the system and potentially cause damage.

Reliability: The probability of a given system performing its mission adequately for a specified period of time under expected operating conditions.

Remote authentication dial-in user service (RADIUS): A server for remote user authentication and accounting. Its primary use is for Internet service providers, though it may as well be used on any network that needs a centralized authentication and/or accounting service for its workstations.

Requirement: A description of a functional or nonfunctional (security) behavior that software or hardware must meet.

Residual risk: The portion of risk that remains after security measures have been applied.

Resilience: The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. In software, a measure of how effectively software can recover after being compromised. If highly

resilient software is compromised, damage to the software will be minimized and it will recover quickly to an acceptable level of service.

RFC: Request for comment. Documents that are the working notes of the Internet research and development community published by the Internet Engineering Task Force (IETF). An RFC document may be on essentially any topic related to computer communication, and can describe methods, protocols, behaviors, and so on pertaining to the Internet.

RFP: Request for proposal. A document issued at an early stage in a procurement process where an organization is invited to submit a proposal to provide goods or services.

RIP: See routing information protocol.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk analysis: The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Risk assessment: The process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure.

Risk management: Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.

Robustness: The degree to which a software component or system can function correctly in the presence of invalid or unexpected inputs and unexpected or stressful environmental conditions, including input and conditions that are intentional and malicious. Robust systems are designed to operate under a variety of conditions within a certain range and will fail gracefully outside of that range. Resilient systems have the ability to recover and adapt to any known environmental changes.

Role: In role-based access control, permitted actions on resources are identified with roles rather than with individual subject identities.

ROM: See read-only memory.

Router: A network component that provides internetworking at the network layer of a network's architecture by allowing individual networks to become part of a wide area network (WAN). A router works by using logical and physical addresses to connect two or more separate networks. It determines the best path by which to send a packet of information.

Routing information protocol (RIP): A common type of routing protocol. RIP bases its routing path on the distance (number of hops) to the destination. RIP maintains optimum routing paths by sending out routing update messages if the network topology changes.

RSA: Rivest, Shamir, and Adleman.

Safeguards: See security safeguards.

Safety: Software or hardware for industrial automation and control systems and IT systems that are life critical should exhibit the property of safety, that is, they should behave as necessary and required even if components of the system fail.

Safety instrumented system (SIS): System used to implement one or more safety instrumented functions. *Note:* A safety instrumented system is composed of any combination of sensors, logic solvers, and actuators.

Safety integrity level: Discrete level (one of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to a safety instrumented system. *Note:* Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

Safety network: Network that connects safety instrumented systems for the communication of safety-related information.

Sandbox: An access control based protection mechanism. It is commonly applied to restrict the access rights of mobile code that is downloaded from a Web site as an applet. The code is set up to run in a "sandbox" that blocks its access to the local workstation's hard disk, thus preventing malicious activity by the code. The sandbox is usually interpreted by a virtual machine such as the Java Virtual Machine (JVM).

Scalar: A computer language variable or field that can hold only one value at a time.

Scanning: Sending packets or requests to another system to gain information to be used in a subsequent attack.

SDLC: See system development life cycle.

Secure coding: The use of software programming practices that reduce or eliminate software defects or programming errors so that software can be built with a higher level of security and quality assurance.

Secure configuration management: The set of procedures that are appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that changes will not lead to violations of the system's security policy.

Secure sockets layer (SSL): A protocol used for protecting private information during transmission via the Internet.

Secure state: A condition in which no subject can access any object in an unauthorized manner.

Security: Measures and controls that ensure the confidentiality, integrity, availability, and accountability of the information processed, transmitted, and stored by industrial automation and control systems or IT systems.

Security evaluation: An evaluation that is performed to assess the degree of trust that can be placed in a system for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is made for the purpose of assessing a system's security safeguards with respect to a specific operational mission; it is a major step in the certification and accreditation process.

Security failure: An event that is a violation of a particular system's explicit or implicit security policy.

Security fault analysis: A security analysis, usually performed on hardware at the gate level, to determine the security properties of a device when a hardware fault is encountered.

Security features: The security-relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards.

Security flaw: An error of commission or omission in a system that might enable protection mechanisms to be bypassed.

Security flow analysis: A security analysis performed on a formal system specification that locates the potential flows of information within the system.

Security functional requirements: Requirements, preferably from the Common Criteria, Part 2, that when taken together specify the security behavior of an industrial automation and control system or IT product or system.

Security kernel: The hardware, firmware, and software elements of a trusted computing base (TCB) that implement the reference monitor concept. The security kernel must mediate all accesses, must be protected from modification, and must be verifiable as correct.

Security level: The combination of a hierarchical classification and a set of nonhierarchical categories that represents the sensitivity of information.

Security measures: Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications.

Security objective: A statement of intent to counter specified threats and/or satisfy specified organizational security policies and assumptions.

Security perimeter: The boundary where security controls are in effect to protect assets.

Security policy: The set of laws, rules, and practices that regulates how an organization manages, protects, and distributes sensitive information.

Security policy model: A formal presentation of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a system manages, protects, and distributes sensitive information. See Bell-LaPadula model and formal security policy model.

Security process: The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system life cycle.

Security requirements: The types and levels of protection that are necessary for equipment, data, information, applications, and facilities to meet the security policy.

Security requirements baseline: A description of the minimum requirements necessary for a system to maintain an acceptable level of security.

Security safeguards: The proactive protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards can include (but are not necessarily limited to) hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices. Also called safeguards.

Security specifications: A detailed description of the safeguards required to protect a system.

Security target (ST): (1) In the Common Criteria, a listing of the security claims for a particular IT security product; (2) A set of security functional and assurance requirements and specifications to be used as the basis for evaluating an identified product or system.

Security test and evaluation (ST&E): Examination and analysis of the safeguards required to protect an IT system, as they have been applied in an operational environment, to determine the security posture of that system. Security posture is the security status of an industrial control and automation system or an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the automation system or enterprise and to react as the situation changes.

Security testing: A process that is used to determine that the security features of a system are implemented as designed. This process includes hands-on functional testing, penetration testing, and verification.

Sensitive information: Information that if lost, misused, modified, or accessed by unauthorized individuals could affect the national interest, industrial automation and control system safety and operations, or IT systems.

Sensitivity label: A piece of information that represents the security level of an object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions.

Sensors and actuators: Measuring elements (sensors) and actuating elements (actuators) connected to process equipment and to the control system.

Service roles: The context in which a software component operates,

consisting of type of service, authentication mechanism, and identities.

Session layer: One of the seven OSI model layers. Establishes, manages, and terminates sessions between applications.

Shared key authentication: A type of authentication that assumes each station has received a secret shared key through a secure channel, independent from an 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of shared key authentication requires implementation of the 802.11 Wired Equivalent Privacy (WEP) algorithm.

Simple mail transfer protocol (SMTP): The Internet email protocol.

Simple Network Management Protocol (SNMP): Internet standard protocol for managing devices on IP computer networks.

Simple security condition: See simple security property.

Simple security property: A Bell-LaPadula security model rule enabling a subject read access to an object only if the security level of the subject dominates the security level of the object. Synonymous with simple security condition.

SLC: See software life cycle.

Social engineering: Attacks targeting an organization's employees through the use of social skills to obtain sensitive information.

Software assurance: The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner.

System development life cycle (SDLC): The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

Software development life cycle process: The process using a model to translate user needs into a software product.

Software engineering: The science and art of specifying, designing,

implementing, and evolving programs, documentation, and operating procedures whereby computers can be made useful to humans.

Software life cycle (SLC): Comprises software concept, requirements analysis, architectural design, detailed design, code construction and unit testing, system testing, release, and code distribution and maintenance.

Software process: A set of activities, methods, and practices that are used to develop and maintain software and associated products.

Software process capability: The range of expected results that can be achieved by following a software process.

Software process maturity: The extent to which a software process is defined, managed, measured, controlled, and effective.

Software process performance: The result achieved by following a software process.

Software security: General-purpose executive, utility, or software development tools and applications programs or routines used to protect data that are handled by a system.

Software system test and evaluation process: A process that plans, develops, and documents the quantitative demonstration of the fulfillment of all baseline functional performance and operational and interface requirements of a software system.

Software weakness: A portion of code that may lead to a vulnerability.

Software-intensive system: A system in which the majority of components and functionalities are implemented in software.

SONET: See synchronous optical networking.

Source code: A series of statements written in a human-readable computer programming language.

Spoofing: Attempting to gain access to a system by posing as an authorized user. Synonymous with impersonating, masquerading, or mimicking.

SQL: See structured query language.

SQL injection: The process of an attacker inserting SQL statements into a query by exploiting vulnerability for the purpose of sending commands to a Web server database.

SSL: See Secure Sockets Layer.

SSO: See system security officer.

ST: See security target.

ST&E: See security test and evaluation.

Standalone (shared system): A system that is physically and electrically isolated from all other systems and intended to be used by more than one person, either simultaneously (e.g., a system that has multiple terminals) or serially, with data belonging to one user remaining available to the system while another user uses the system (e.g., a personal computer that has nonremovable storage media, such as a hard disk).

Standalone (single-user system): A system that is physically and electrically isolated from all other systems and is intended to be used by one person at a time, with no data belonging to other users remaining in the system (e.g., a personal computer that has removable storage media, such as a flash drive).

Star property (* property): A Bell-LaPadula security model rule giving a subject write access to an object only if the security level of the object dominates the security level of the subject. Also called the confinement property.

State variable: A variable that represents either the state of the system or the state of some system resource.

Structured query language (SQL): An international standard for defining and accessing relational databases.

Subject: An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or that changes the system state.

Subversion: An intentional violation of software's integrity or its security

controls in order to compromise the software or the using system.

Supervisor state: Synonymous with executive state.

Survivability: The capability of software or hardware to fulfill its objectives in the presence of attacks, failures, or accidents.

Symmetric (private) key encryption: Cryptographic system in which the sender and receiver both know a secret key that is used to encrypt and decrypt a message.

Synchronous optical networking (SONET): A fiber-optic transmission system for high-speed digital traffic. SONET is part of the Broadband Integrated Services Digital Network (BISDN) standard.

Synchronous transmission: A type of communications data synchronization whereby frames are sent within defined time periods. It uses a clock to control the timing of bits being sent in a frame. See asynchronous transmission.

System: Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.

System development methodologies: Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.

System entity: A system subject (user or process) or object.

System integrity: A characteristic of a system that performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. Also see integrity.

Security mode: The lowest security level supported by a system at a particular time or in a particular environment.

System security officer (SSO): Individual having the responsibility to ensure the security of an industrial automation and control system or IT system, excluding, for example, guards, physical security personnel, law enforcement officials, and disaster recovery officials.

System testing: A type of testing that verifies the installation of the entire network. Testers normally complete system testing in a simulated production environment, simulating actual users in order to ensure that the network meets all stated requirements.

Tainted input: Input data that has not been examined or sanitized prior to use by an application.

Tampering: Any unauthorized modification that alters the proper functioning of equipment or a system in a manner that degrades the security or functionality that it provides.

Target of evaluation (TOE): In the Common Criteria, TOE refers to the product to be tested.

TCB: See trusted computing base.

TCP: See Transmission Control Protocol.

Technical attack: An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users through social engineering.

Technical vulnerability: A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in a risk to the owner, user, or manager of the system.

TELNET (not an acronym): A virtual terminal protocol used in the Internet, enabling users to log in to a remote host. TELNET is defined as part of the TCP/IP protocol suite.

TEMPEST: Transient ElectroMagnetic Pulse Emanations Standard, the U.S. government standard for control of spurious compromising emanations emitted by electrical equipment; also used to refer to the investigation, study, and control of such emanations.

Test case: An executable test with a specific set of input values and a corresponding expected result.

Threat agent: A means of exploiting a vulnerability in a system, operation, or facility.

Threat analysis: The examination of all actions and events that might adversely affect a system or operation.

Threat: Any circumstance or event with the potential to cause harm to an industrial automation and control system or IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Threat factor: The characterization of a threat based on a violation of confidentiality, integrity, or availability (CIA); the asset being targeted, the role of the user, and type of accessibility. It helps refine the application context to aid in analyzing the threat.

Threat monitoring: The analysis, assessment, and review of audit trails and other data that are collected for the purpose of searching for system events that might constitute violations or attempted violations of system security.

TLS: See transport layer security.

TOE: See target of evaluation.

Top-level specification: A nonprocedural description of system behavior at the most abstract level; typically, a functional specification that omits all implementation details.

Topology: A description of a network's geographical layout of nodes and links.

Traceroute: Software utility used to determine the path to a target computer.

Transmission Control Protocol (TCP): A commonly used protocol for establishing and maintaining communications between applications on different computers. TCP provides full-duplex, acknowledged, and flow-controlled service to upper-layer protocols and applications.

Transmission Control Protocol / Internet Protocol (TCP/IP): A de facto industry-standard protocol for interconnecting disparate networks. TCP and IP are standard protocols that define both the reliable full-duplex transport level and the connectionless, best-effort unit of information passed across a network such as the Internet.

Transport layer: OSI model layer that provides mechanisms for the establishment, maintenance, and orderly termination of virtual circuits while shielding the higher layers from the network implementation details.

Transport layer security (TLS): An authentication and security protocol widely implemented in browsers and Web servers.

Trap door: A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in a manner that appears innocent—for example, a special “random” key sequence at a terminal. Software developers often introduce trap doors in their code to enable them to re-enter the system and perform certain functions.

Trojan horse: A computer program that has an apparently or actually useful function but contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity.

True positive: When a security tool reports a weakness that is actually present. See false positive, false negative.

Trust: In a relationship between entities, the confidence that each entity will behave as expected, dependably, securely, and reliably within a specified context.

Trusted computer system: A system that employs sufficient hardware and software security assurance measures to enable its use for the simultaneous processing of a range of sensitive or classified information.

Trusted computing base (TCB): The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a unified security policy depends solely on the mechanisms within the TCB and on the correct input of parameters by system administrative personnel (e.g., a user’s clearance level) related to the security policy.

Trusted distribution: A method for distributing the TCB hardware, software, and firmware components, both originals and updates, that provides means for protecting the TCB from modification during distribution and for the detection of any changes to the TCB that might occur.

Trusted path: A mechanism by which a person at a terminal can communicate directly with the TCB. This mechanism can be activated only by the person or by the TCB and cannot be imitated by untrusted software.

Trusted process: A process whose incorrect or malicious execution is capable of violating system security policy.

Trusted software: The software portion of the TCB.

Trustworthiness: The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

UDP: See User Datagram Protocol.

Unit: See lines, units, cells.

Untrusted process: A process that has not been evaluated or examined for adherence to the security policy. It might include incorrect or malicious code that attempts to circumvent the security mechanisms.

Use case: A technique for capturing potential functional requirements that employs the use of one or more scenarios that convey how the system should interact with the end user or another system to achieve a specific goal.

Note: Use cases typically treat the system as a black box, and the interactions with the system, including system responses, are as perceived from outside the system. Use cases are popular because they simplify the description of requirements and avoid the problem of making assumptions about how this functionality will be accomplished.

User: (1) A person or process that is accessing an industrial automation and control system or IT system either by direct connection (e.g., via terminals) or by indirect connection (in other words, preparing input data or receiving output that is not reviewed for content or classification by a responsible individual); (2) A person or process authorized to access an industrial automation and control system or IT system.

User Datagram Protocol (UDP): UDP uses the underlying Internet Protocol (IP) to transport a message. This is an unreliable, connectionless delivery scheme. It does not use acknowledgments to ensure that messages arrive and does not provide feedback to control the rate of information flow. UDP messages can be lost, duplicated, or arrive out of order. It is useful in sending high volumes of data such as streaming video.

User ID: A unique symbol or character string that is used by a system to identify a specific user.

Validation: A process for evaluating whether software will satisfy the specified requirements (functional and nonfunctional) for its intended purpose.

Verification: A process for evaluating whether software conforms to the specifications, regulations, or other conditions imposed on it while it was being developed.

Verification and validation (V&V): All of the verification and validation activities that are undertaken to ensure that software will function according to its specification.

Virus: A self-replicating or self-reproducing program that spreads by inserting copies of itself into other executable code or documents.

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability analysis: A method of determining vulnerability that includes the susceptibility of a particular system to a specific attack and the opportunities that are available to a threat agent to mount that attack.

Vulnerability assessment: Systematic examination of an industrial automation and control system or IT system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Weakness: A bug found in software that has the potential of being exploited as a vulnerability when the software is operational.

White box test: A test in which the ethical hacking team has full knowledge of the target information system.

White hat hacker: An individual who conducts ethical hacking to help secure and protect and organization's information systems.

Wide area network (WAN): A network that interconnects users over a wide area, usually encompassing different metropolitan areas.

Wired equivalency privacy (WEP): The algorithm of the IEEE 802.11 wireless LAN standard that is used to protect transmitted information from

disclosure. WEP is designed to prevent the violation of the confidentiality of data transmitted over a wireless LAN. WEP generates secret shared encryption keys that both source and destination stations use to alter frame bits to avoid disclosure to eavesdroppers. WEP is no longer considered a viable encryption mechanism due to known weaknesses.

Wired equivalency privacy (WEP) encryption: An encryption method specified in the IEEE 802.11 standard for wireless security. See Wired Equivalency Privacy (WEP).

Wireless: A property of a computing device whereby it can access a network without a wired connection.

WLAN: Wireless local area network.

Work factor: An estimate of the effort or time needed by a potential intruder who has specified expertise and resources to overcome a protective measure.

Work function: The difficulty of recovering plaintext from ciphertext, as measured by cost and/or time. The security of the system is directly proportional to the value of the work function. The work function need only be large enough to suffice for the intended application. If the message to be protected loses its value after a short period of time, the work function need only be large enough to ensure that the decryption would be highly infeasible in that period of time.

Write: A fundamental operation that results only in the flow of information from a subject to an object.

Write access: Permission to write to an object.

Zeroizing: The act of erasing sensitive parameters from a cryptographic module.

Zeroization: The practice of erasing sensitive parameters (especially keys) from a cryptographic module to prevent their disclosure. The keys are typically zeroized (erased) in response to an attempt to tamper with the module.

Bibliography

ANSI/ISA-51.1-1979 (R1993) “Process Instrumentation Terminology.”

ANSI/ISA-75.05.01-2000 (R2005) “Control Valve Terminology.”

ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) “Functional Safety: Safety Instrumented Systems for the Process Industry Sector.”

ANSI/ISA-88.01-2010 (IEC 62264-1 Mod) “Batch Control Part 1: Models and Terminology.”

ANSI/ISA-95.00.01-2010 “Enterprise-Control System Integration, Part 1: Models and Terminology.”

ANSI/ISA-99.00.01-2007 “Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts and Models.”

ANSI/ISA-99.02.01-2009 “Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.”

ANSI/ISA-TR99.00.01-2007 “Security for Industrial Automation and Control Systems, Technical Report 1: Security Technologies for Industrial Automation and Control Systems.”

Bailey, D. and Wright, E. *Practical SCADA for Industry*. Milpitas (CA): IDC Technologies, 2003.

Boyer, S. *SCADA Supervisory Control and Data Acquisition, 2nd Edition*. Research Triangle Park: ISA, 1999.

Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration (CMMI) for Software Engineering, v1.1*. Pittsburgh: Carnegie Mellon University, 2002.

Committee on National Security Systems (CNSS) CNSS Instruction No. 4009,

“National Information Assurance (IA) Glossary.” Washington, DC: CNSS, April 2010.

Erickson, K. and Hedrick, J. *Plant Wide Process Control*. Hoboken: John Wiley & Sons, 1999.

Falco, Joe, et al. *IT Security for Industrial Control Systems*. NIST IR 6859, 2003 at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=821684.

Federal Information Processing Standards (FIPS) PUB 140-2 *Security Requirements for Cryptographic Modules* “Section 2, Glossary of Terms and Acronyms.” Washington, DC: U.S. National Institute of Standards and Technology, 2001.

FIPS PUB 199 *Standards for Security Categorization of Federal Information and Information Systems*. Washington, DC: U.S. National Institute of Standards and Technology, 2004.

FIPS PUB 200 *Minimum Security Requirements for Federal Information and Information Systems*. Washington, DC: U.S. National Institute of Standards and Technology, 2006.

IEC/PAS 62409 “Real-time Ethernet for Plant Automation, ed 1.0” (2005).

IEC/PAS 62410 “Real-time Ethernet SERCOS III, ed. 1.0” (2005).

International Electrotechnical Commission (IEC) *Glossary* at <http://std.iec.ch/glossary>. Geneva: IEC.

International Society of Automation *The Automation, Systems, and Instrumentation Dictionary, 4th Edition*. Research Triangle Park: ISA, 2003.

ISA-dTR62443-1-2, “Security for Industrial Automation and Control Systems - Master Glossary of Terms and Abbreviations,” 2011.

ISA-d99.02.02 “Security for Industrial Automation and Control Systems: Operating an Industrial Automation and Control System Security Program.”

ISA-d99.03.01, “Security for industrial automation and control systems: Target security levels.”

ISA-d99.03.02, “Security for industrial automation and control systems: System security compliance.”

ISA-d99.03.03, “Security for industrial automation and control systems: Technical security requirements for industrial automation and control systems.”

ISO/IEC 10746-1:1998 “Information technology – Open Distributed Processing – Reference model: Overview.”

ISO/IEC 15408-1:2009 “Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.”

ISO/IEC 15408-2:2008 “Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.”

ISO/IEC 15408-3:2008 “Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.”

ISO/IEC 17799:2005 “Information technology – Security techniques – Code of practice for information security management.”

ISO/IEC 27001:2005 “Information technology – Security techniques – Information security management systems – Requirements.”

ISO/IEC 7498-2:1989 “Information processing systems – Open System Interconnection – Basic reference Model – Part 2: Security Architecture.”

NIST Process Control Security Requirements Forum (PCSRF), Industrial Control System-System Protection Profile (ICS-SPP), Version 1.0, Washington, DC: National Institute of Science and Technology, 2004.

NIST SP 800-18 Revision 1 “Guide for Developing Security Plans for Federal Information Systems,” Washington, DC: National Institute of Science and Technology, 2006.

NIST SP 800-28 “Guidelines on Active Content and Mobile Code,” Version 2, Washington, DC: National Institute of Science and Technology, 2008.

NIST SP 800-30 “Risk Management Guide for Information Technology Systems” Washington, DC: National Institute of Science and Technology, 2002.

NIST SP 800-30 Revision 1, “DRAFT Guide for Conducting Risk Assessments,” Washington, DC: National Institute of Science and Technology, 2011.

NIST SP 800-34 “Contingency Planning Guide for Information Technology Systems, Revision 1,” Washington, DC: National Institute of Science and Technology, 2010.

NIST SP 800-37 “Guide for Applying the Risk Management Framework to Federal Information Systems, Revision 1,” Washington, DC: National Institute of Science and Technology, 2010.

NIST SP 800-47 “Security Guide for Interconnecting Information Technology Systems,” Washington, DC: National Institute of Science and Technology, 2002.

NIST SP 800-53 Revision 3 “Recommended Security Controls for Federal Information Systems.” Washington, DC: National Institute of Science and Technology, 2010.

NIST SP 800-61 “Computer Security Incident Handling Guide, Revision 2(Draft)” Washington, DC: National Institute of Science and Technology, 2012.

NIST SP 800-82 “Guide to Industrial Control Systems (ICS) Security,” Washington, DC: National Institute of Science and Technology, 2011.

NIST SP 800-137 “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” Washington, DC: National Institute of Science and Technology, 2011.